



Informatica (Version 9.6.1 HotFix 2)

Administrator Guide

Copyright (c) 1993-2016 Informatica LLC. All rights reserved.

This software and documentation contain proprietary information of Informatica Corporation and are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright law. Reverse engineering of the software is prohibited. No part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without prior consent of Informatica Corporation. This Software may be protected by U.S. and/or international Patents and other Patents Pending.

Use, duplication, or disclosure of the Software by the U.S. Government is subject to the restrictions set forth in the applicable software license agreement and as provided in DFARS 227.7202-1(a) and 227.7702-3(a) (1995), DFARS 252.227-7013^(c)(1)(ii) (OCT 1988), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14 (ALT III), as applicable.

The information in this product or documentation is subject to change without notice. If you find any problems in this product or documentation, please report them to us in writing.

Informatica, Informatica Platform, Informatica Data Services, PowerCenter, PowerCenterRT, PowerCenter Connect, PowerCenter Data Analyzer, PowerExchange, PowerMart, Metadata Manager, Informatica Data Quality, Informatica Data Explorer, Informatica B2B Data Transformation, Informatica B2B Data Exchange Informatica On Demand, Informatica Identity Resolution, Informatica Application Information Lifecycle Management, Informatica Complex Event Processing, Ultra Messaging and Informatica Master Data Management are trademarks or registered trademarks of Informatica Corporation in the United States and in jurisdictions throughout the world. All other company and product names may be trade names or trademarks of their respective owners.

Portions of this software and/or documentation are subject to copyright held by third parties, including without limitation: Copyright DataDirect Technologies. All rights reserved. Copyright © Sun Microsystems. All rights reserved. Copyright © RSA Security Inc. All Rights Reserved. Copyright © Ordinal Technology Corp. All rights reserved. Copyright © Aandacht c.v. All rights reserved. Copyright Genivia, Inc. All rights reserved. Copyright Isomorphic Software. All rights reserved. Copyright © Meta Integration Technology, Inc. All rights reserved. Copyright © Intalio. All rights reserved. Copyright © Oracle. All rights reserved. Copyright © Adobe Systems Incorporated. All rights reserved. Copyright © DataArt, Inc. All rights reserved. Copyright © ComponentSource. All rights reserved. Copyright © Microsoft Corporation. All rights reserved. Copyright © Rogue Wave Software, Inc. All rights reserved. Copyright © Teradata Corporation. All rights reserved. Copyright © Yahoo! Inc. All rights reserved. Copyright © Glyph & Cog, LLC. All rights reserved. Copyright © Thinkmap, Inc. All rights reserved. Copyright © Clearpace Software Limited. All rights reserved. Copyright © Information Builders, Inc. All rights reserved. Copyright © OSS Nokalva, Inc. All rights reserved. Copyright Edifecs, Inc. All rights reserved. Copyright Cleo Communications, Inc. All rights reserved. Copyright © International Organization for Standardization 1986. All rights reserved. Copyright © ej-technologies GmbH. All rights reserved. Copyright © Jaspersoft Corporation. All rights reserved. Copyright © International Business Machines Corporation. All rights reserved. Copyright © yWorks GmbH. All rights reserved. Copyright © Lucent Technologies. All rights reserved. Copyright (c) University of Toronto. All rights reserved. Copyright © Daniel Veillard. All rights reserved. Copyright © Unicode, Inc. Copyright IBM Corp. All rights reserved. Copyright © MicroQuill Software Publishing, Inc. All rights reserved. Copyright © PassMark Software Pty Ltd. All rights reserved. Copyright © LogiXML, Inc. All rights reserved. Copyright © 2003-2010 Lorenzi Davide, All rights reserved. Copyright © Red Hat, Inc. All rights reserved. Copyright © The Board of Trustees of the Leland Stanford Junior University. All rights reserved. Copyright © EMC Corporation. All rights reserved. Copyright © Flexera Software. All rights reserved. Copyright © Jinfonet Software. All rights reserved. Copyright © Apple Inc. All rights reserved. Copyright © Telerik Inc. All rights reserved. Copyright © BEA Systems. All rights reserved. Copyright © PDFlib GmbH. All rights reserved. Copyright © Orientation in Objects GmbH. All rights reserved. Copyright © Tanuki Software, Ltd. All rights reserved. Copyright © Ricebridge. All rights reserved. Copyright © Sencha, Inc. All rights reserved. Copyright © Scalable Systems, Inc. All rights reserved. Copyright © jqWidgets. All rights reserved.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>), and/or other software which is licensed under various versions of the Apache License (the "License"). You may obtain a copy of these Licenses at <http://www.apache.org/licenses/>. Unless required by applicable law or agreed to in writing, software distributed under these Licenses is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the Licenses for the specific language governing permissions and limitations under the Licenses.

This product includes software which was developed by Mozilla (<http://www.mozilla.org/>), software copyright The JBoss Group, LLC, all rights reserved; software copyright © 1999-2006 by Bruno Lowagie and Paulo Soares and other software which is licensed under various versions of the GNU Lesser General Public License Agreement, which may be found at <http://www.gnu.org/licenses/lgpl.html>. The materials are provided free of charge by Informatica, "as-is", without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

The product includes ACE(TM) and TAO(TM) software copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University, Copyright (©) 1993-2006, all rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (copyright The OpenSSL Project. All Rights Reserved) and redistribution of this software is subject to terms available at <http://www.openssl.org> and <http://www.openssl.org/source/license.html>.

This product includes Curl software which is Copyright 1996-2013, Daniel Stenberg, <daniel@haxx.se>. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at <http://curl.haxx.se/docs/copyright.html>. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

The product includes software copyright 2001-2005 (©) MetaStuff, Ltd. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at <http://www.dom4j.org/license.html>.

The product includes software copyright © 2004-2007, The Dojo Foundation. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at <http://dojotoolkit.org/license>.

This product includes ICU software which is copyright International Business Machines Corporation and others. All rights reserved. Permissions and limitations regarding this software are subject to terms available at <http://source.icu-project.org/repos/icu/icu/trunk/license.html>.

This product includes software copyright © 1996-2006 Per Bothner. All rights reserved. Your right to use such materials is set forth in the license which may be found at <http://www.gnu.org/software/kawa/Software-License.html>.

This product includes OSSP UUID software which is Copyright © 2002 Ralf S. Engelschall, Copyright © 2002 The OSSP Project Copyright © 2002 Cable & Wireless Deutschland. Permissions and limitations regarding this software are subject to terms available at <http://www.opensource.org/licenses/mit-license.php>.

This product includes software developed by Boost (<http://www.boost.org/>) or under the Boost software license. Permissions and limitations regarding this software are subject to terms available at http://www.boost.org/LICENSE_1_0.txt.

This product includes software copyright © 1997-2007 University of Cambridge. Permissions and limitations regarding this software are subject to terms available at <http://www.pcre.org/license.txt>.

This product includes software copyright © 2007 The Eclipse Foundation. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at <http://www.eclipse.org/org/documents/epl-v10.php> and at <http://www.eclipse.org/org/documents/edl-v10.php>.

This product includes software licensed under the terms at <http://www.tcl.tk/software/tcltk/license.html>, <http://www.bosrup.com/web/overlib/?License>, <http://www.stlport.org/doc/license.html>, <http://asm.ow2.org/license.html>, <http://www.cryptix.org/LICENSE.TXT>, <http://hsqldb.org/web/hsqldbLicense.html>, <http://httpunit.sourceforge.net/doc/license.html>, <http://jung.sourceforge.net/license.txt>, http://www.gzip.org/zlib/zlib_license.html, <http://www.openldap.org/software/release/>

license.html, <http://www.libssh2.org>, <http://slf4j.org/license.html>, <http://www.sente.ch/software/OpenSourceLicense.html>, <http://fusesource.com/downloads/license-agreements/fuse-message-broker-v-5-3- license-agreement>; <http://antlr.org/license.html>; <http://aopalliance.sourceforge.net/>; <http://www.bouncycastle.org/licence.html>; <http://www.jgraph.com/jgraphdownload.html>; <http://www.jcraft.com/jsch/LICENSE.txt>; http://jotm.objectweb.org/bsd_license.html; . <http://www.w3.org/Consortium/Legal/2002/copyright-software-20021231>; <http://www.slf4j.org/license.html>; <http://nanoxml.sourceforge.net/orig/copyright.html>; <http://www.json.org/license.html>; <http://forge.ow2.org/projects/javaservice/>; <http://www.postgresql.org/about/licence.html>; <http://www.sqlite.org/copyright.html>; <http://www.tcl.tk/software/tcltk/license.html>; <http://www.jaxen.org/faq.html>; <http://www.jdom.org/docs/faq.html>; <http://www.slf4j.org/license.html>; <http://www.iodbc.org/dataspace/iodbc/wiki/ODBC/License>; <http://www.keplerproject.org/md5/license.html>; <http://www.toedter.com/en/jcalendar/license.html>; <http://www.edankert.com/bounce/index.html>; <http://www.net-snmpp.org/about/license.html>; <http://www.openmdx.org/#FAQ>; http://www.php.net/license/3_01.txt; <http://srp.stanford.edu/license.txt>; <http://www.schneier.com/blowfish.html>; <http://www.jmock.org/license.html>; <http://xsom.java.net>; <http://benalman.com/about/license/>; <https://github.com/CreateJS/EaselJS/blob/master/src/easeljs/display/Bitmap.js>; <http://www.h2database.com/html/license.html#summary>; <http://jsoncpp.sourceforge.net/LICENSE>; <http://jdbc.postgresql.org/license.html>; <http://protobuf.googlecode.com/svn/trunk/src/google/protobuf/descriptor.proto>; <https://github.com/rantav/hector/blob/master/LICENSE>; <http://web.mit.edu/Kerberos/krb5-current/doc/mitK5license.html>; <http://jibx.sourceforge.net/jibx-license.html>; <https://github.com/lyokato/libgeohash/blob/master/LICENSE>; <https://github.com/hjiang/jsonxx/blob/master/LICENSE>; <https://code.google.com/p/lz4/>; <https://github.com/jedisct1/libsodium/blob/master/LICENSE>; <http://one-jar.sourceforge.net/index.php?page=documents&file=license>; <https://github.com/EsotericSoftware/kryo/blob/master/license.txt>; <http://www.scala-lang.org/license.html>; <https://github.com/tinkerpop/blueprints/blob/master/LICENSE.txt>; and <http://gee.cs.oswego.edu/dl/classes/EDU/oswego/cs/dl/util/concurrent/intro.html>.

This product includes software licensed under the Academic Free License (<http://www.opensource.org/licenses/afl-3.0.php>), the Common Development and Distribution License (<http://www.opensource.org/licenses/cddl1.php>) the Common Public License (<http://www.opensource.org/licenses/cpl1.0.php>), the Sun Binary Code License Agreement Supplemental License Terms, the BSD License (<http://www.opensource.org/licenses/bsd-license.php>), the new BSD License (<http://opensource.org/licenses/BSD-3-Clause>), the MIT License (<http://www.opensource.org/licenses/mit-license.php>), the Artistic License (<http://www.opensource.org/licenses/artistic-license-1.0>) and the Initial Developer's Public License Version 1.0 (<http://www.firebirdsql.org/en/initial-developer-s-public-license-version-1-0/>).

This product includes software copyright © 2003-2006 Joe Walnes, 2006-2007 XStream Committers. All rights reserved. Permissions and limitations regarding this software are subject to terms available at <http://xstream.codehaus.org/license.html>. This product includes software developed by the Indiana University Extreme! Lab. For further information please visit <http://www.extreme.indiana.edu/>.

This product includes software Copyright (c) 2013 Frank Balluffi and Markus Moeller. All rights reserved. Permissions and limitations regarding this software are subject to terms of the MIT license.

This Software is protected by U.S. Patent Numbers 5,794,246; 6,014,670; 6,016,501; 6,029,178; 6,032,158; 6,035,307; 6,044,374; 6,092,086; 6,208,990; 6,339,775; 6,640,226; 6,789,096; 6,823,373; 6,850,947; 6,895,471; 7,117,215; 7,162,643; 7,243,110; 7,254,590; 7,281,001; 7,421,458; 7,496,588; 7,523,121; 7,584,422; 7,676,516; 7,720,842; 7,721,270; 7,774,791; 8,065,266; 8,150,803; 8,166,048; 8,166,071; 8,200,622; 8,224,873; 8,271,477; 8,327,419; 8,386,435; 8,392,460; 8,453,159; 8,458,230; 8,707,336; 8,886,617 and RE44,478, International Patents and other Patents Pending.

DISCLAIMER: Informatica Corporation provides this documentation "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of noninfringement, merchantability, or use for a particular purpose. Informatica Corporation does not warrant that this software or documentation is error free. The information provided in this software or documentation may include technical inaccuracies or typographical errors. The information in this software and documentation is subject to change at any time without notice.

NOTICES

This Informatica product (the "Software") includes certain drivers (the "DataDirect Drivers") from DataDirect Technologies, an operating company of Progress Software Corporation ("DataDirect") which are subject to the following terms and conditions:

1. THE DATADIRECT DRIVERS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.
2. IN NO EVENT WILL DATADIRECT OR ITS THIRD PARTY SUPPLIERS BE LIABLE TO THE END-USER CUSTOMER FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR OTHER DAMAGES ARISING OUT OF THE USE OF THE ODBC DRIVERS, WHETHER OR NOT INFORMED OF THE POSSIBILITIES OF DAMAGES IN ADVANCE. THESE LIMITATIONS APPLY TO ALL CAUSES OF ACTION, INCLUDING, WITHOUT LIMITATION, BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS.

Part Number: IN-ADG-96100-HF2-0001

Table of Contents

Preface	15
Informatica Resources.	15
Informatica My Support Portal.	15
Informatica Documentation.	15
Informatica Product Availability Matrixes.	15
Informatica Web Site.	15
Informatica How-To Library.	16
Informatica Knowledge Base.	16
Informatica Support YouTube Channel.	16
Informatica Marketplace.	16
Informatica Velocity.	16
Informatica Global Customer Support.	16
 Chapter 1: Understanding Domains.....	 17
Understanding Domains Overview.	17
Nodes.	18
Gateway Nodes.	18
Worker Nodes.	18
Service Manager.	18
Application Services.	19
Analyst Service.	20
Content Management Service.	21
Data Integration Service.	21
Metadata Manager Service.	21
Model Repository Service.	21
PowerCenter Integration Service.	21
PowerCenter Repository Service.	22
PowerExchange Listener Service.	22
PowerExchange Logger Service.	22
Reporting Service.	22
Reporting and Dashboards Service.	23
SAP BW Service.	23
Web Services Hub.	23
High Availability.	23
Informatica Data Usage Policy.	23
Configuring Informatica DiscoveryIQ Proxy Details.	24
Disabling Informatica Data Usage.	24
 Chapter 2: Managing Your Account.....	 25
Managing Your Account Overview.	25

Log In to Informatica Administrator.	25
Informatica Administrator URL.	26
Troubleshooting the Login to Informatica Administrator.	26
Password Management.	27
Changing Your Password.	27
Editing Preferences.	27
Preferences.	27
Informatica MySupport Portal Credentials.	28
Enter Informatica MySupport Portal Credentials.	28
Searching Informatica Knowledge Base.	28
Chapter 3: Using Informatica Administrator.	29
Using Informatica Administrator Overview.	29
Domain Tab Overview.	30
Domain Tab - Services and Nodes View.	30
Domain.	32
Folders.	32
Application Services.	33
Nodes.	37
Grids.	37
Licenses.	37
Domain Tab - Connections View.	38
Logs Tab.	38
Reports Tab.	39
Monitoring Tab.	39
Security Tab.	39
Using the Search Section.	40
Using the Security Navigator.	40
Groups.	41
Users.	41
Roles.	42
Service States.	42
Process States.	42
Job States.	44
Keyboard Shortcuts.	45
Chapter 4: Domain Management.	46
Domain Management Overview.	46
Alert Management.	47
Configuring SMTP Settings.	47
Subscribing to Alerts.	48
Viewing Alerts.	48
Folder Management.	49

Creating a Folder.	49
Moving Objects to a Folder.	50
Removing a Folder	50
Domain Security Management.	50
User Security Management.	51
Application Service Management.	51
Enabling and Disabling Services and Service Processes.	52
Viewing Service Processes.	53
Configuring Restart for Service Processes.	53
Removing Application Services.	53
Troubleshooting Application Services.	54
Node Management.	54
Defining and Adding Nodes.	54
Configuring Node Properties.	55
Viewing Processes on the Node.	57
Shutting Down and Restarting the Node.	58
Removing the Node Association.	59
Removing a Node.	59
Gateway Configuration.	59
Domain Configuration Management.	60
Backing Up the Domain Configuration.	61
Restoring the Domain Configuration.	61
Migrating the Domain Configuration.	61
Updating the Domain Configuration Database Connection.	63
Domain Tasks.	64
Managing and Monitoring Application Services and Nodes.	64
Viewing Dependencies for Application Services, Nodes, and Grids.	65
Shutting Down a Domain.	66
Domain Properties.	67
General Properties.	67
Database Properties.	68
Gateway Configuration Properties.	69
Service Level Management.	70
SMTP Configuration.	70
Custom Properties for the Domain.	71
Chapter 5: High Availability.	72
High Availability Overview.	72
Resilience.	73
Application Client Resilience.	73
Application Service Resilience.	74
Node Resilience.	74
Example Resilience Timeout Configuration.	74

Restart and Failover.	75
Domain Failover.	76
Application Service Restart and Failover.	76
Recovery.	77
Configuration for a Highly Available Domain.	77
Application Service Resilience Configuration.	78
Application Service Failover Configuration.	79
PowerCenter Integration Service Failover and Recovery Configuration.	79
Command Line Program Resilience Configuration.	80
Domain Failover Configuration.	80
Node Restart Configuration.	81
Troubleshooting High Availability.	81
Chapter 6: Connections.	82
Connections Overview.	82
Connection Management.	82
Creating a Connection.	83
Refreshing the Connections List.	83
Viewing a Connection.	84
Configuring Pooling for a Connection.	84
Editing and Testing a Connection.	84
Deleting a Connection.	85
Pass-through Security.	85
Pass-Through Security with Data Object Caching.	86
Adding Pass-Through Security	86
Pooling Properties in Connection Objects.	87
Chapter 7: Connection Properties.	88
Adabas Connection Properties.	88
DataSift Connection Properties.	90
Facebook Connection Properties.	91
Greenplum Connection Properties.	92
HBase Connection Properties.	94
HDFS Connection Properties.	95
Hive Connection Properties.	96
HTTP Connection Properties.	101
IBM DB2 Connection Properties.	103
IBM DB2 for i5/OS Connection Properties.	105
IBM DB2 for z/OS Connection Properties.	108
IMS Connection Properties.	111
JDBC Connection Properties.	114
LinkedIn Connection Properties.	117
MS SQL Server Connection Properties.	117

ODBC Connection Properties.	120
Oracle Connection Properties.	121
Salesforce Connection Properties.	123
SAP Connection Properties.	124
Sequential Connection Properties.	126
Teradata Parallel Transporter Connection Properties.	128
Twitter Connection Properties.	130
Twitter Streaming Connection Properties.	131
VSAM Connection Properties.	132
Web Content-Kapow Katalyst Connection Properties.	134
Web Services Connection Properties.	135
Chapter 8: Domain Object Export and Import.	138
Domain Object Export and Import Overview.	138
Export Process.	138
Rules and Guidelines for Exporting Domain Objects.	139
View Domain Objects.	139
Viewable Domain Object Names.	140
Import Process.	146
Rules and Guidelines for Importing Domain Objects.	146
Conflict Resolution.	146
Chapter 9: License Management.	148
License Management Overview.	148
License Validation.	149
Licensing Log Events.	149
License Management Tasks.	149
Types of License Keys.	150
Original Keys.	150
Incremental Keys.	150
Creating a License Object.	151
Assigning a License to a Service.	152
Rules and Guidelines for Assigning a License to a Service.	152
Unassigning a License from a Service.	152
Updating a License.	153
Removing a License.	153
License Properties.	154
License Details.	154
Supported Platforms.	155
Repositories.	155
Service Options.	156
Connections.	156
Metadata Exchange Options.	156

Chapter 10: Log Management.....	157
Log Management Overview.	157
Log Manager Architecture.	158
PowerCenter Session and Workflow Log Events.	158
Log Manager Recovery.	159
Troubleshooting the Log Manager.	159
Log Location.	159
Log Management Configuration.	160
Purging Log Events.	160
Time Zone.	160
Configuring Log Management Properties.	161
Using the Logs Tab.	161
Viewing Log Events.	161
Configuring Log Columns.	163
Saving Log Events.	164
Exporting Log Events.	164
Viewing Administrator Tool Log Errors.	166
Log Events.	166
Log Event Components.	166
Domain Log Events.	167
Analyst Service Log Events.	168
Data Integration Service Log Events.	168
Listener Service Log Events.	168
Logger Service Log Events.	168
Model Repository Service Log Events.	169
Metadata Manager Service Log Events.	169
PowerCenter Integration Service Log Events.	169
PowerCenter Repository Service Log Events.	169
Reporting Service Log Events.	170
SAP BW Service Log Events.	170
Web Services Hub Log Events.	170
User Activity Log Events.	171
Log Aggregator.	171
Aggregating Application Service Logs.	172
Processing Aggregated Application Service Logs.	172
 Chapter 11: Monitoring.....	 173
Monitoring Overview.	173
Navigator in the Monitoring Tab.	174
Views in the Monitoring Tab.	175
Statistics in the Monitoring Tab.	175
Reports on the Monitoring Tab.	176

Monitoring Setup.	178
Step 1. Configure Global Settings.	179
Step 2. Configure Monitoring Preferences.	180
Monitor Data Integration Services	180
Properties View for a Data Integration Service.	180
Reports View for a Data Integration Service.	181
Monitor Jobs.	181
Viewing Logs for a Job.	182
Canceling a Job.	182
Monitor Applications.	182
Properties View for an Application.	182
Reports View for an Application.	183
Monitor Deployed Mapping Jobs.	183
Viewing Logs for a Deployed Mapping Job.	183
Reissuing a Deployed Mapping Job.	183
Canceling a Deployed Mapping Job.	184
Monitor Logical Data Objects.	184
Properties View for a Logical Data Object.	184
Cache Refresh Runs View for a Logical Data Object.	184
Viewing Logs for Data Object Cache Refresh Runs.	185
Monitor SQL Data Services.	185
Properties View for an SQL Data Service.	185
Connections View for an SQL Data Service.	186
Requests View for an SQL Data Service.	186
Virtual Tables View for an SQL Data Service.	187
Reports View for an SQL Data Service.	188
Monitor Web Services.	188
Properties View for a Web Service.	188
Reports View for a Web Service.	189
Operations View for a Web Service.	189
Requests View for a Web Service.	189
Monitor Workflows.	189
Workflow Graph	190
View Workflow Objects.	190
Workflow States.	191
Workflow Object States.	192
Mapping Task Work Item States.	194
Canceling or Aborting a Workflow.	195
Workflow Recovery.	195
Recovering a Workflow.	196
Workflow Logs.	196
Monitoring a Folder of Objects.	198

Viewing the Context of an Object.	198
Configuring the Date and Time Custom Filter.	199
Configuring the Elapsed Time Custom Filter.	199
Configuring the Multi-Select Custom Filter.	199
Monitoring an Object.	199
Chapter 12: Domain Reports.	200
Domain Reports Overview.	200
License Management Report.	200
Licensing.	201
CPU Summary.	201
CPU Detail.	202
Repository Summary.	203
User Summary.	203
User Detail.	203
Hardware Configuration.	204
Node Configuration.	205
Licensed Options.	205
Running the License Management Report.	205
Sending the License Management Report in an Email.	206
Web Services Report.	207
Understanding the Web Services Report.	207
General Properties and Web Services Hub Summary.	209
Web Services Historical Statistics.	209
Web Services Run-time Statistics.	210
Web Service Properties.	211
Web Service Top IP Addresses.	211
Web Service Historical Statistics Table.	211
Running the Web Services Report.	212
Running the Web Services Report for a Secure Web Services Hub.	212
Chapter 13: Node Diagnostics.	214
Node Diagnostics Overview.	214
Informatica MySupport Portal Login.	215
Logging In to the Informatica MySupport Portal.	215
Generating Node Diagnostics.	216
Downloading Node Diagnostics.	216
Uploading Node Diagnostics.	217
Analyzing Node Diagnostics.	218
Identify Bug Fixes.	218
Identify Recommendations.	218

Chapter 14: Understanding Globalization.....	219
Globalization Overview.	219
Unicode.	220
Working with a Unicode PowerCenter Repository.	220
Locales.	221
System Locale.	221
User Locale.	222
Input Locale.	222
Data Movement Modes.	222
Character Data Movement Modes.	222
Changing Data Movement Modes.	223
Code Page Overview.	224
UNIX Code Pages.	225
Windows Code Pages.	225
Choosing a Code Page.	226
Code Page Compatibility.	226
Domain Configuration Database Code Page.	227
Administrator Tool Code Page.	228
PowerCenter Client Code Page.	228
PowerCenter Integration Service Process Code Page.	228
PowerCenter Repository Code Page.	229
Metadata Manager Repository Code Page.	229
PowerCenter Source Code Page.	229
PowerCenter Target Code Page.	230
Command Line Program Code Pages.	230
Code Page Compatibility Summary.	231
Code Page Validation.	233
Relaxed Code Page Validation.	234
Configuring the PowerCenter Integration Service.	235
Selecting Compatible Source and Target Code Pages.	235
Troubleshooting for Code Page Relaxation.	235
PowerCenter Code Page Conversion.	236
Choosing Characters for PowerCenter Repository Metadata.	236
Case Study: Processing ISO 8859-1 Data.	237
The ISO 8859-1 Environment.	237
Configuring the ISO 8859-1 Environment.	237
Case Study: Processing Unicode UTF-8 Data.	239
The UTF-8 Environment.	239
Configuring the UTF-8 Environment.	240
 Chapter 15: Informatica Cloud Administration.....	 242
Informatica Cloud Administration Overview	242

Informatica Cloud Organizations	242
Informatica Cloud Organization Properties.	243
Adding an Organization.	243
Removing an Organization.	243
Editing Informatica Cloud Login Credentials.	243
Informatica Cloud Secure Agent.	244
Informatica Cloud Connections.	244
Appendix A: Code Pages.	245
Supported Code Pages for Application Services.	245
Supported Code Pages for Sources and Targets.	247
Appendix B: Command Line Privileges and Permissions.	257
infacmd as Commands.	257
infacmd dis Commands.	258
infacmd ipc Commands.	259
infacmd isp Commands.	260
infacmd mrs Commands.	271
infacmd ms Commands.	272
infacmd oie Commands.	272
infacmd ps Commands.	272
infacmd pwx Commands.	273
infacmd rtm Commands.	274
infacmd sql Commands.	275
infacmd rds Commands.	276
infacmd wfs Commands.	276
pmcmd Commands.	276
pmrep Commands.	278
Appendix C: Custom Roles.	284
PowerCenter Repository Service Custom Roles.	284
Metadata Manager Service Custom Roles.	286
Reporting Service Custom Roles.	287
Test Data Manager Service Custom Roles.	294
Analyst Service Custom Role.	297
Appendix D: Informatica Platform Connectivity.	298
Informatica Platform Connectivity Overview.	298
Domain Connectivity.	299
Model Repository Connectivity.	300
PowerCenter Connectivity.	301
Repository Service Connectivity.	303
Integration Service Connectivity.	303

PowerCenter Client Connectivity.	304
Reporting Service and Metadata Manager Service Connectivity.	305
Native Connectivity.	306
ODBC Connectivity.	306
JDBC Connectivity.	307
Appendix E: Configure the Web Browser.	308
Configure the Web Browser.	308
Appendix F: Security Concepts.	309
What is a group?.	309
What is a user?.	309
What is a role?.	310
What is a privilege?.	310
What is an operating system profile?.	310
Index.	311

Preface

The *Informatica Administrator Guide* is written for Informatica users. It contains information you need to manage the domain. The *Informatica Administrator Guide* assumes you have basic working knowledge of Informatica.

Informatica Resources

Informatica My Support Portal

As an Informatica customer, you can access the Informatica My Support Portal at <http://mysupport.informatica.com>.

The site contains product information, user group information, newsletters, access to the Informatica customer support case management system (ATLAS), the Informatica How-To Library, the Informatica Knowledge Base, Informatica Product Documentation, and access to the Informatica user community.

Informatica Documentation

The Informatica Documentation team makes every effort to create accurate, usable documentation. If you have questions, comments, or ideas about this documentation, contact the Informatica Documentation team through email at infa_documentation@informatica.com. We will use your feedback to improve our documentation. Let us know if we can contact you regarding your comments.

The Documentation team updates documentation as needed. To get the latest documentation for your product, navigate to Product Documentation from <http://mysupport.informatica.com>.

Informatica Product Availability Matrixes

Product Availability Matrixes (PAMs) indicate the versions of operating systems, databases, and other types of data sources and targets that a product release supports. You can access the PAMs on the Informatica My Support Portal at <https://mysupport.informatica.com/community/my-support/product-availability-matrices>.

Informatica Web Site

You can access the Informatica corporate web site at <http://www.informatica.com>. The site contains information about Informatica, its background, upcoming events, and sales offices. You will also find product and partner information. The services area of the site includes important information about technical support, training and education, and implementation services.

Informatica How-To Library

As an Informatica customer, you can access the Informatica How-To Library at <http://mysupport.informatica.com>. The How-To Library is a collection of resources to help you learn more about Informatica products and features. It includes articles and interactive demonstrations that provide solutions to common problems, compare features and behaviors, and guide you through performing specific real-world tasks.

Informatica Knowledge Base

As an Informatica customer, you can access the Informatica Knowledge Base at <http://mysupport.informatica.com>. Use the Knowledge Base to search for documented solutions to known technical issues about Informatica products. You can also find answers to frequently asked questions, technical white papers, and technical tips. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team through email at KB_Feedback@informatica.com.

Informatica Support YouTube Channel

You can access the Informatica Support YouTube channel at <http://www.youtube.com/user/INFASupport>. The Informatica Support YouTube channel includes videos about solutions that guide you through performing specific tasks. If you have questions, comments, or ideas about the Informatica Support YouTube channel, contact the Support YouTube team through email at supportvideos@informatica.com or send a tweet to @INFASupport.

Informatica Marketplace

The Informatica Marketplace is a forum where developers and partners can share solutions that augment, extend, or enhance data integration implementations. By leveraging any of the hundreds of solutions available on the Marketplace, you can improve your productivity and speed up time to implementation on your projects. You can access Informatica Marketplace at <http://www.informaticamarketplace.com>.

Informatica Velocity

You can access Informatica Velocity at <http://mysupport.informatica.com>. Developed from the real-world experience of hundreds of data management projects, Informatica Velocity represents the collective knowledge of our consultants who have worked with organizations from around the world to plan, develop, deploy, and maintain successful data management solutions. If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at ips@informatica.com.

Informatica Global Customer Support

You can contact a Customer Support Center by telephone or through the Online Support.

Online Support requires a user name and password. You can request a user name and password at <http://mysupport.informatica.com>.

The telephone numbers for Informatica Global Customer Support are available from the Informatica web site at <http://www.informatica.com/us/services-and-training/support-services/global-support-centers/>.

CHAPTER 1

Understanding Domains

This chapter includes the following topics:

- [Understanding Domains Overview, 17](#)
- [Nodes, 18](#)
- [Service Manager, 18](#)
- [Application Services, 19](#)
- [High Availability, 23](#)
- [Informatica Data Usage Policy, 23](#)

Understanding Domains Overview

Informatica has a service-oriented architecture that provides the ability to scale services and share resources across multiple machines. High availability functionality helps minimize service downtime due to unexpected failures or scheduled maintenance in the Informatica environment.

The Informatica domain is the fundamental administrative unit in Informatica. The domain supports the administration of the distributed services. A domain is a collection of nodes and services that you can group in folders based on administration ownership.

A node is the logical representation of a machine in a domain. One node in the domain acts as a gateway to receive service requests from clients and route them to the appropriate service and node. Services and processes run on nodes in a domain. The availability of a service or process on a node depends on how you configure the service and the node.

Services for the domain include the Service Manager and a set of application services:

- **Service Manager.** A service that manages all domain operations. It runs the application services and performs domain functions on each node in the domain. Some domain functions include authentication, authorization, and logging.
- **Application Services.** Services that represent server-based functionality, such as the Model Repository Service and the Data Integration Service. The application services that run on a node depend on the way you configure the services.

The Service Manager and application services control security. The Service Manager manages users and groups that can log in to application clients and authenticates the users who log in to the application clients. The Service Manager and application services authorize user requests from application clients.

Informatica Administrator (the Administrator tool), consolidates the administrative tasks for domain objects such as services, nodes, licenses, and grids. You manage the domain and the security of the domain through the Administrator tool.

If you have the PowerCenter high availability option, you can scale services and eliminate single points of failure for services. Services can continue running despite temporary network or hardware failures.

Nodes

During installation, you add the installation machine to the domain as a node. You can add multiple nodes to a domain. Each node in the domain runs a Service Manager that manages domain operations on that node. The operations that the Service Manager performs depend on the type of node. A node can be a gateway node or a worker node. You can subscribe to alerts to receive notification about node events such as node failure or a master gateway election. You can also generate and upload node diagnostics to the Configuration Support Manager and review information such as available EBFs and Informatica recommendations.

Gateway Nodes

A gateway node is any node that you configure to serve as a gateway for the domain. One node acts as the gateway at any given time. That node is called the master gateway. A gateway node can run application services, and it can serve as a master gateway node. The master gateway node is the entry point to the domain.

The Service Manager on the master gateway node performs all domain operations on the master gateway node. The Service Managers running on other gateway nodes perform limited domain operations on those nodes.

You can configure more than one node to serve as a gateway. If the master gateway node becomes unavailable, the Service Manager on other gateway nodes elect another master gateway node. If you configure one node to serve as the gateway and the node becomes unavailable, the domain cannot accept service requests.

Worker Nodes

A worker node is any node not configured to serve as a gateway. A worker node can run application services, but it cannot serve as a gateway. The Service Manager performs limited domain operations on a worker node.

Service Manager

The Service Manager is a service that manages all domain operations. It runs within Informatica services. It runs as a service on Windows and as a daemon on UNIX. When you start Informatica services, you start the Service Manager.

The Service Manager runs on each node. If the Service Manager is not running, the node is not available.

The Service Manager runs on all nodes in the domain to support application services and the domain:

- **Application service support.** The Service Manager on each node starts application services configured to run on that node. It starts and stops services and service processes based on requests from clients. It also directs service requests to application services. The Service Manager uses TCP/IP to communicate with the application services.

- **Domain support.** The Service Manager performs functions on each node to support the domain. The functions that the Service Manager performs on a node depend on the type of node. For example, the Service Manager running on the master gateway node performs all domain functions on that node. The Service Manager running on any other node performs some domain functions on that node.

The following table describes the domain functions that the Service Manager performs:

Function	Description
Alerts	The Service Manager sends alerts to subscribed users. You subscribe to alerts to receive notification for node failure and master gateway election on the domain, and for service process failover for services on the domain. When you subscribe to alerts, you receive notification emails.
Authentication	The Service Manager authenticates users who log in to application clients. Authentication occurs on the master gateway node.
Authorization	The Service Manager authorizes user requests for domain objects based on the privileges, roles, and permissions assigned to the user. Requests can come from the Administrator tool. Domain authorization occurs on the master gateway node. Some application services authorize user requests for other objects.
Domain Configuration	The Service Manager manages the domain configuration metadata. Domain configuration occurs on the master gateway node.
Node Configuration	The Service Manager manages node configuration metadata in the domain. Node configuration occurs on all nodes in the domain.
Licensing	The Service Manager registers license information and verifies license information when you run application services. Licensing occurs on the master gateway node.
Logging	The Service Manager provides accumulated log events from each service in the domain and for sessions and workflows. To perform the logging function, the Service Manager runs a Log Manager and a Log Agent. The Log Manager runs on the master gateway node. The Log Agent runs on all nodes where the PowerCenter Integration Service runs.
User Management	The Service Manager manages the native and LDAP users and groups that can log in to application clients. It also manages the creation of roles and the assignment of roles and privileges to native and LDAP users and groups. User management occurs on the master gateway node.
Monitoring	The Service Manager persists, updates, retrieves, and publishes run-time statistics for integration objects in the Model repository. The Service Manager stores the monitoring configuration in the domain configuration repository.

Application Services

Application services represent server-based functionality. Application services include the following services:

- Analyst Service
- Content Management Service

- Data Integration Service
- Metadata Manager Service
- Model Repository Service
- PowerCenter Integration Service
- PowerCenter Repository Service
- PowerExchange Listener Service
- PowerExchange Logger Service
- Reporting Service
- Reporting and Dashboards Service
- Test Data Manager Service
- SAP BW Service
- Web Services Hub

When you configure an application service, you designate a node to run the service process. When a service process runs, the Service Manager assigns a port number from the range of port numbers assigned to the node.

The service process is the runtime representation of a service running on a node. The service type determines how many service processes can run at a time. For example, the PowerCenter Integration Service can run multiple service processes at a time when you run it on a grid.

If you have the high availability option, you can run a service on multiple nodes. Designate the primary node to run the service. All other nodes are backup nodes for the service. If the primary node is not available, the service runs on a backup node. You can subscribe to alerts to receive notification in the event of a service process failover.

If you do not have the high availability option, configure a service to run on one node. If you assign multiple nodes, the service will not start.

Analyst Service

The Analyst Service is an application service that runs the Informatica Analyst application in the Informatica domain. The Analyst Service manages the connections between service components and the users that log in to Informatica Analyst. The Analyst Service connects to a Data Integration Service, a Model Repository Service, a Metadata Manager Service, and a Search Service. The Analyst Service also specifies a flat file cache directory and a directory for business glossary export files.

When you configure the Analyst Service, connect it to a Data Integration Service to run profiles, scorecards, and mapping specifications. You can also connect the Analyst Service to a Data Integration Service that runs Human tasks. Connect the Analyst Service to a Model Repository Service to identify a Model repository.

Connect the Analyst Service to a Metadata Manager Service to perform data lineage operations on scorecards in the Analyst tool. Connect the Analyst Service to a Search Service to manage search operations in the Analyst tool.

Specify a flat file cache directory to store temporary data from flat files that you upload. Specify a business glossary directory to stores temporary files that you export from the Business Glossary.

Content Management Service

The Content Management Service is an application service that manages reference data. It provides reference data information to the Data Integration Service and to the Developer tool.

The Content Management Service provides reference data properties to the Data Integration Service. The Data Integration Service uses these properties when it runs mappings that require address reference data.

The Content Management Service also provides Developer tool transformations with information about the address reference data and identity populations installed in the file system. The Developer tool displays the installed address reference datasets in the Content Status view within application preferences. The Developer tool displays the installed identity populations in the Match transformation and Comparison transformation.

Data Integration Service

The Data Integration Service is an application service that performs data integration tasks for Informatica Analyst, Informatica Developer, and external clients. Data integration tasks include previewing data and running profiles, SQL data services, web services, and mappings.

When you start a command from the command line or an external client to run SQL data services and mappings in an application, the command sends the request to the Data Integration Service.

Metadata Manager Service

The Metadata Manager Service is an application service that runs the Metadata Manager application and manages connections between the Metadata Manager components.

Use Metadata Manager to browse and analyze metadata from disparate source repositories. You can load, browse, and analyze metadata from application, business intelligence, data integration, data modelling, and relational metadata sources.

You can configure the Metadata Manager Service to run on only one node. The Metadata Manager Service is not a highly available service. However, you can run multiple Metadata Manager Services on the same node.

Model Repository Service

The Model Repository Service is an application service that manages the Model repository. The Model repository is a relational database that stores the metadata for projects created in Informatica Analyst and Informatica Developer. The Model repository also stores run-time and configuration information for applications that are deployed to a Data Integration Service.

You can configure the Model Repository Service to run on one node. The Model Repository Service is not a highly available service. However, you can run multiple Model Repository Services on the same node. If the Model Repository Service fails, it automatically restarts on the same node.

PowerCenter Integration Service

The PowerCenter Integration Service runs PowerCenter sessions and workflows. When you configure the PowerCenter Integration Service, you can specify where you want it to run:

- On a grid. When you configure the service to run on a grid, it can run on multiple nodes at a time. The PowerCenter Integration Service dispatches tasks to available nodes assigned to the grid. If you do not have the high availability option, the task fails if any service process or node becomes unavailable. If you have the high availability option, failover and recovery is available if a service process or node becomes unavailable.

- On nodes. If you have the high availability option, you can configure the service to run on multiple nodes. By default, it runs on the primary node. If the primary node is not available, it runs on a backup node. If the service process fails or the node becomes unavailable, the service fails over to another node. If you do not have the high availability option, you can configure the service to run on one node.

PowerCenter Repository Service

The PowerCenter Repository Service manages the PowerCenter repository. It retrieves, inserts, and updates metadata in the repository database tables. If the service process fails or the node becomes unavailable, the service fails.

If you have the high availability option, you can configure the service to run on primary and backup nodes. By default, the service process runs on the primary node. If the service process fails, a new process starts on the same node. If the node becomes unavailable, a service process starts on one of the backup nodes.

PowerExchange Listener Service

The PowerExchange Listener Service is an application service that manages the PowerExchange Listener. The PowerExchange Listener manages communication between a PowerCenter or PowerExchange client and a data source for bulk data movement and change data capture. The PowerCenter Integration Service connects to the PowerExchange Listener through the Listener Service. Use the Administrator tool to manage the service and view service logs.

If you have the PowerCenter high availability option, you can run the Listener Service on multiple nodes. If the Listener Service process fails on the primary node, it fails over to a backup node.

PowerExchange Logger Service

The Logger Service is an application service that manages the PowerExchange Logger for Linux, UNIX, and Windows. The PowerExchange Logger captures change data from a data source and writes the data to PowerExchange Logger log files. Use the Administrator tool to manage the service and view service logs.

If you have the PowerCenter high availability option, you can run the Logger Service on multiple nodes. If the Logger Service process fails on the primary node, it fails over to a backup node.

Reporting Service

The Reporting Service is an application service that runs the Data Analyzer application in an Informatica domain. You log in to Data Analyzer to create and run reports on data in a relational database or to run the following PowerCenter reports: PowerCenter Repository Reports, Data Profiling Reports, or Metadata Manager Reports. You can also run other reports within your organization.

The Reporting Service is not a highly available service. However, you can run multiple Reporting Services on the same node.

Configure a Reporting Service for each data source you want to run reports against. If you want a Reporting Service to point to different data sources, create the data sources in Data Analyzer.

Reporting and Dashboards Service

You can create the Reporting and Dashboards Service from Informatica Administrator. You can use the service to create and run reports from the JasperReports application.

JasperReports is an open source reporting library that users can embed into any Java application. JasperReports Server builds on JasperReports and forms a part of the Jaspersoft Business Intelligence suite of products.

SAP BW Service

The SAP BW Service listens for RFC requests from SAP NetWeaver BI and initiates workflows to extract from or load to SAP NetWeaver BI. The SAP BW Service is not highly available. You can configure it to run on one node.

Web Services Hub

The Web Services Hub receives requests from web service clients and exposes PowerCenter workflows as services. The Web Services Hub does not run an associated service process. It runs within the Service Manager.

High Availability

High availability is an option that eliminates a single point of failure in a domain and provides minimal service interruption in the event of failure. High availability consists of the following components:

- Resilience. The ability of application services to tolerate transient network failures until either the resilience timeout expires or the external system failure is fixed.
- Failover. The migration of an application service or task to another node when the node running the service process becomes unavailable.
- Recovery. The automatic completion of tasks after a service is interrupted. Automatic recovery is available for PowerCenter Integration Service and PowerCenter Repository Service tasks. You can also manually recover PowerCenter Integration Service workflows and sessions. Manual recovery is not part of high availability.

Informatica Data Usage Policy

Informatica DiscoveryIQ is a monitoring tool that sends routine reports on data usage and system statistics to Informatica Global Customer Support.

Informatica DiscoveryIQ uploads data to Informatica 15 minutes after you install and configure Informatica domain. Thereafter, the domain sends the data every 30 days. Data collection and upload is enabled by default. You can choose to not send any usage statistics to Informatica.

If the network where you install Informatica services need a proxy server to communicate with the external network, configure proxy details.

Informatica DiscoveryIQ enables Informatica Global Customer Support to provide an environment health check after the analysis of system statistics and domain reports. You can receive best practices and recommendations from Informatica Global Customer Support based on the reports. The usage statistics provide Informatica a proactive insight into product implementation.

Informatica DiscoveryIQ reports the following data to Informatica:

- Operating system details
- CPU information
- Informatica license key serial number
- Gateway information
- Domain options
- Node options
- Application service information

Configuring Informatica DiscoveryIQ Proxy Details

Configure proxy server details if the network on which you install Informatica services use a proxy server to communicate with the external network.

1. In the Administrator tool header area, click **Manage > DiscoveryIQ Proxy Details**.
2. Enter the domain, host name, and port number of the proxy server.
3. Enter the user name and password to connect to the proxy server.
4. Click **OK** to save the proxy server details.

Disabling Informatica Data Usage

You can disable the upload of usage data from the Informatica domain in the Administrator tool.

1. In the Administrator tool, click **Help > About**.
2. Click **Data Usage Policy**.
3. Clear **Enable Usage Collection**.
4. Click **OK**.

CHAPTER 2

Managing Your Account

This chapter includes the following topics:

- [Managing Your Account Overview, 25](#)
- [Log In to Informatica Administrator, 25](#)
- [Password Management, 27](#)
- [Editing Preferences, 27](#)
- [Preferences, 27](#)
- [Informatica MySupport Portal Credentials, 28](#)

Managing Your Account Overview

Manage your account to change your password or edit user preferences.

If you have a native user account, you can change your password at any time with the Change Password application. If someone else created your user account, change your password the first time you log in to the Administrator tool.

User preferences control the options that appear in the Administrator tool when you log in. User preferences do not affect the options that appear when another user logs in to the Administrator tool.

You can configure Informatica MySupport Portal credentials for your account so that you can access the Informatica Knowledge Base from the Administrator tool.

Log In to Informatica Administrator

You must have a user account to log in to the Informatica Administrator web application.

If the Informatica domain runs on a network with Kerberos authentication, you must configure the browser to allow access to the Informatica web applications. In Microsoft Internet Explorer and Google Chrome, add the URL of the Informatica web application to the list of trusted sites. If you are using Chrome version 41 or later, you must also set the `AuthServerWhitelist` and `AuthNegotiateDelegateWhitelist` policies.

1. Start a Microsoft Internet Explorer or Google Chrome browser.
2. In the **Address** field, enter the URL for the Administrator tool:

- If the Administrator tool is not configured to use a secure connection, enter the following URL:

`http://<fully qualified hostname>:<http port>`

- If the Administrator tool is configured to use a secure connection, enter the following URL:

`https://<fully qualified hostname>:<http port>`

Host name and port in the URL represent the host name and port number of the master gateway node. If you configured secure communication for the domain, you must use HTTPS in the URL to ensure that you can access the Administrator tool.

If you use Kerberos authentication, the network uses single sign on. You do not need to log in to the Administrator tool with a user name and password.

3. If you do not use Kerberos authentication, enter the user name, password, and security domain for your user account, and then click **Login**.

The **Security Domain** field appears when the Informatica domain contains an LDAP security domain. If you do not know the security domain that your user account belongs to, contact the Informatica domain administrator.

Note: If this is the first time you log in with the user name and password provided by the domain administrator, change your password to maintain security.

Informatica Administrator URL

In the Administrator tool URL, `<host>:<port>` represents the host name of the master gateway node and the Administrator tool port number.

You configure the Administrator tool port when you define the domain. You can define the domain during installation or by running the *infasetup* DefineDomain command line program. If you enter the domain port instead of the Administrator tool port in the URL, the browser is directed to the Administrator tool port.

Note: If the domain fails over to a different master gateway node, the host name in the Administrator tool URL is equal to the host name of the elected master gateway node.

Troubleshooting the Login to Informatica Administrator

If the Informatica domain uses Kerberos authentication, you might encounter the following issues when logging in to the Administrator tool:

I cannot log in to the Administrator tool from the same machine where I created the domain gateway node.

After installation, if you cannot log in to the Administrator tool from the same machine where you created the domain gateway node, clear the browser cache. When you initially log in to the Administrator tool after installation, you can only log in with the Administrator user account created during installation. If a different user credential is stored in the browser cache, the login can fail.

A blank page appears after I log in to the Administrator tool.

If a blank page appears after you log in to the Administrator tool, verify that you enabled delegation for all user accounts with service principals used in the Informatica domain. To enable delegation, in the Microsoft Active Directory Service, set the **Trust this user for delegation to any service (Kerberos only)** option for each user account that you set an SPN.

Password Management

You can change the password through the Change Password application.

You can open the Change Password application from the Administrator tool or with the following URL:

`http://<host>:<port>/passwordchange`

The Service Manager uses the user password associated with a worker node to authenticate the domain user. If you change a user password that is associated with one or more worker nodes, the Service Manager updates the password for each worker node. The Service Manager cannot update nodes that are not running. For nodes that are not running, the Service Manager updates the password when the nodes restart.

Note: For an LDAP user account, change the password in the LDAP directory service.

Changing Your Password

Change the password for a native user account at any time. For a user account created by someone else, change the password the first time you log in to the Administrator tool.

1. In the Administrator tool header area, click **Manage > Change Password**.
The Change Password application opens in a new browser window.
2. Enter the current password in the **Password** box, and the new password in the **New Password** and **Confirm Password** boxes.
3. Click **Update**.

Editing Preferences

Edit your preferences to determine the options that appear in the Administrator tool when you log in.

1. In the Administrator tool header area, click **Manage > Preferences**.
The **Preferences** window appears.
2. Click **Edit**.
The **Edit Preferences** dialog box appears.

Preferences

Your preferences determine the options that appear in the Administrator tool when you log in. Your preferences do not affect the options that appear when another user logs in to the Administrator tool.

The following table describes the options that you can configure for your preferences:

Option	Description
Subscribe for Alerts	Subscribes you to domain and service alerts. You must have a valid email address configured for your user account. Default is No.
Show Custom Properties	Displays custom properties in the contents panel when you click an object in the Navigator. You use custom properties to configure Informatica behavior for special cases or to increase performance. Hide the custom properties to avoid inadvertently changing the values. Use custom properties only if Informatica Global Customer Support instructs you to.

Informatica MySupport Portal Credentials

You can enter your Informatica MySupport Portal credentials in the Administrator tool to access the Informatica Knowledge Base from the Administrator tool.

You can also view the search results for an error message in the Informatica Knowledge Base by clicking the error message code in the Administrator tool.

Enter Informatica MySupport Portal Credentials

Enter your Informatica MySupport Portal credentials to access the Informatica Knowledge Base from the Administrator tool.

1. Click **Manage > Support Portal Credentials**.
The **Edit Informatica MySupport Portal Login Credentials** window appears.
2. Enter your Informatica MySupport Portal credentials and the customer project ID.
3. Click **OK**.

Searching Informatica Knowledge Base

You can search for terms in the Informatica Knowledge Base directly from the Administrator tool.

1. Click **Help > Search Knowledge Base**.
The **Search Knowledge Base** window appears.
2. Enter the term that you want to search in the text box.
3. Click **OK**.
The search results appear in a different browser window.

CHAPTER 3

Using Informatica Administrator

This chapter includes the following topics:

- [Using Informatica Administrator Overview, 29](#)
- [Domain Tab Overview, 30](#)
- [Domain Tab - Services and Nodes View, 30](#)
- [Domain Tab - Connections View, 38](#)
- [Logs Tab, 38](#)
- [Reports Tab, 39](#)
- [Monitoring Tab, 39](#)
- [Security Tab, 39](#)
- [Service States, 42](#)
- [Process States, 42](#)
- [Job States, 44](#)
- [Keyboard Shortcuts, 45](#)

Using Informatica Administrator Overview

Informatica Administrator is the administration tool that you use to administer the Informatica domain and Informatica security.

Use the Administrator tool to complete the following types of tasks:

Domain administrative tasks

Manage logs, domain objects, user permissions, and domain reports. Generate and upload node diagnostics. Monitor jobs and applications that run on the Data Integration Service. Domain objects include application services, nodes, grids, folders, database connections, operating system profiles, and licenses.

Security administrative tasks

Manage users, groups, roles, and privileges.

The Administrator tool has the following tabs:

Domain

View and edit the properties of the domain and objects within the domain.

Logs

View log events for the domain and services within the domain.

Monitoring

View the status of profile jobs, preview jobs, mapping jobs, SQL data services, and web services for each Data Integration Service.

Monitoring

View the status of profile jobs, scorecard jobs, preview jobs, mapping jobs, SQL data services, web services, and workflows for each Data Integration Service.

Reports

Run a Web Services Report or License Management Report.

Security

Manage users, groups, roles, and privileges.

The Administrator tool has the following header items:

Log out

Log out of the Administrator tool.

Manage

Manage your account.

Help

Access help for the current tab and determine the Informatica version.

Domain Tab Overview

On the **Domain** tab, you can view information about the domain and view and manage objects in the domain.

The contents that appear and the tasks you can complete on the **Domain** tab vary based on the view that you select. You can select the following views:

- **Services and Nodes.** View and manage application services and nodes.
- **Connections.** View and manage connections.

You can configure the appearance of these views.

Domain Tab - Services and Nodes View

The **Services and Nodes** view shows all application services and nodes defined in the domain.

The **Services and Nodes** view has the following components:

Navigator

Appears in the left pane of the **Domain** tab. The Navigator displays the following types of objects:

- **Domain.** You can view one domain, which is the highest object in the Navigator hierarchy.

- **Folders.** Use folders to organize domain objects in the Navigator. Select a folder to view information about the folder and the objects in the folder.
- **Application services.** An application service represents server-based functionality. Select an application service to view information about the service and its processes.
- **Nodes.** A node represents a machine in the domain. You assign resources to nodes and configure service processes to run on nodes.
- **Grids.** Create a grid to run the Data Integration Service or PowerCenter Integration Service on multiple nodes. Select a grid to view nodes assigned to the grid.
- **Licenses.** Create a license on the **Domain** tab based on a license key file provided by Informatica. Select a license to view services assigned to the license.

Contents panel

Appears in the right pane of the **Domain** tab and displays information about the domain or domain object that you select in the Navigator.

Actions menu in the Navigator

When you select the domain in the Navigator, you can create a folder, service, node, grid, or license.

When you select a domain object in the Navigator, you can delete the object, move it to a folder, or refresh the object.

Actions menu on the Domain tab

When you select the domain in the Navigator, you shut down or view logs for the domain.

When you select a node in the Navigator, you can remove a node association, recalculate the CPU profile benchmark, or shut down the node.

When you select a service in the Navigator, you can recycle or disable the service, view back up files in or back up the repository contents, manage the repository domain, notify users, and view logs.

When you select a license in the Navigator, you can add an incremental key to the license.

Domain

You can view one domain in the **Services and Nodes** view on the **Domain** tab. It is the highest object in the Navigator hierarchy.

When you select the domain in the Navigator, the contents panel shows the following views and buttons, which enable you to complete the following tasks:

- **Overview** view. View all application services, nodes, and grids in the domain, organized by object type. You can view statuses of application services and nodes and information about grids. You can also view dependencies among application services, nodes, and grids, and view properties about domain objects. You can also recycle application services.

Click an application service to see its name, version, status, and the statuses of its individual processes. Click a node to see its name, status, the number of service processes running on the node, and the name of any grids to which the node belongs. Click a grid to see the name of the grid, the number of service processes running in the grid, and the names of the nodes in the grid. The statuses are available, disabled, and unavailable.

By default, the **Overview** view shows an abbreviation of each domain object's name. Click the **Show Details** button to show the full names of the objects. Click the **Hide Details** button to show abbreviations of the object names.

To view the dependencies among application services, nodes, and grids, right-click an object and click **View Dependency**. The **View Dependency** graph appears.

To view properties for an application service, node, or grid, right-click an object and click **View Properties**. The contents panel shows the object properties.

To recycle an application service, right-click a service and click **Recycle Service**.

- Click an application service to see its name, description, status, and the statuses of its individual processes. Click a node to see the name, status and the number of service processes running on the node.

By default, the **Overview** view shows an abbreviation of each domain object's name. Click the **Show Details** button to show the full names of the objects. Click the **Hide Details** button to show abbreviations of the object names.

- **Properties** view. View or edit domain resilience properties.
- **Resources** view. View available resources for each node in the domain.
- **Permissions** view. View or edit group and user permissions on the domain.
- **Diagnostics** view. View node diagnostics, generate and upload node diagnostics to Customer Support Manager, or edit customer portal login details.
- **Plug-ins** view. View plug-ins registered in the domain.
- **View Logs for Domain** button. View logs for the domain and services within the domain.

In the **Actions** menu in the Navigator, you can add a node, grid, application service, or license to the domain. You can also add folders, which you use to organize domain objects.

In the **Actions** menu on the **Domain** tab, you can shut down, view logs, or access help on the current view.

Folders

You can use folders in the domain to organize objects and to manage security.

Folders can contain nodes, services, grids, licenses, and other folders.

When you select a folder in the Navigator, the Navigator opens to display the objects in the folder. The contents panel displays the following information:

- **Overview** view. Displays services in the folder and the nodes where the service processes run.
- **Properties** view. Displays the name and description of the folder.
- **Permissions** view. View or edit group and user permissions on the folder.

In the **Actions** menu in the Navigator, you can delete the folder, move the folder into another folder, refresh the contents on the **Domain** tab, or access help on the current tab.

Application Services

Application services are a group of services that represent Informatica server-based functionality.

In the **Services and Nodes** view on the **Domain** tab, you can create and manage the following application services:

Analyst Service

Runs Informatica Analyst in the Informatica domain. The Analyst Service manages the connections between service components and the users that log in to Informatica Analyst.

The Analyst Service connects to a Data Integration Service, a Model Repository Service, a Metadata Manager Service, and a Search Service. The Analyst Service also specifies a flat file cache directory and a directory for business glossary export files.

You can create and recycle the Analyst Service in the Informatica domain to access the Analyst tool. You can launch the Analyst tool from the Administrator tool.

When you select an Analyst Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node. The contents panel also displays the URL of the Analyst Service instance.
- **Properties** view. Manage general, model repository, data integration, metadata manager, flat file cache, business glossary export, logging, and custom properties.
- **Processes** view. View and edit service process properties on each assigned node.
- **Permissions** view. View or edit the group and user permissions on the Analyst Service.
- **Actions** menu. Manage the service and repository contents.

Content Management Service

Manages reference data and compiles rule specifications into mapplets. Stores properties for address reference data and identity population data.

When you select a Content Management Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node.
- **Properties** view. Manage general, master, data integration, model repository, logging, and custom properties.
- **Processes** view. View and edit service process properties on each assigned node.
- **Permissions** view. View or edit the group and user permissions on the Content Management Service.
- **Actions** menu. Manage the service.

Data Integration Service

Completes data integration tasks for Informatica Analyst, Informatica Developer, and external clients. When you preview or run data profiles, SQL data services, and mappings in Informatica Analyst or Informatica Developer, the application sends requests to the Data Integration Service to perform the data integration tasks. When you start a command from the command line or an external client to run SQL data services and mappings in an application, the command sends the request to the Data Integration Service.

When you select a Data Integration Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node.
- **Properties** view. Manage general, model repository, logging, logical data object and virtual table cache, profiling, data object cache, and custom properties. Set the default deployment option.
- **Processes** view. View and edit service process properties on each assigned node.
- **Applications** view. Start and stop applications and SQL data services. Back up applications. Manage application properties.
- **Actions** menu. Manage the service and repository contents.

Metadata Manager Service

Runs the Metadata Manager application and manages connections between the Metadata Manager components.

When you select a Metadata Manager Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node. The contents panel also displays the URL of the Metadata Manager Service instance.
- **Properties** view. View or edit Metadata Manager properties.
- **Associated Services** view. View and configure the Integration Service associated with the Metadata Manager Service.
- **Permissions** view. View or edit the group and user permissions on the Metadata Manager Service.
- **Actions** menu. Manage the service and repository contents.

Model Repository Service

Manages the Model repository. The Model repository stores metadata created by Informatica products, such as Informatica Developer, Informatica Analyst, the Data Integration Service, and Informatica Administrator. The Model repository enables collaboration among the products.

When you select a Model Repository Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node.
- **Properties** view. Manage general, repository database, search, and custom properties.
- **Processes** view. View and edit service process properties on each assigned node.
- **Actions** menu. Manage the service and repository contents.

PowerCenter Integration Service

Runs PowerCenter sessions and workflows. Select a PowerCenter Integration Service in the Navigator to access information about the service.

When you select a PowerCenter Integration Service in the Navigator, the contents panel displays the following information:

- Service and service processes status. View the status of the service and the service process for each node.
- **Properties** view. View or edit Integration Service properties.
- **Associated Repository** view. View or edit the repository associated with the Integration Service.
- **Processes** view. View or edit the service process properties on each assigned node.
- **Permissions** view. View or edit group and user permissions on the Integration Service.
- **Actions** menu. Manage the service.

PowerCenter Repository Service

Manages the PowerCenter repository. It retrieves, inserts, and updates metadata in the repository database tables. Select a PowerCenter Repository Service in the Navigator to access information about the service.

When you select a PowerCenter Repository Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process for each node. The service status also displays the operating mode for the PowerCenter Repository Service. The contents panel also displays a message if the repository has no content or requires upgrade.
- **Properties** view. Manage general and advanced properties, node assignments, and database properties.
- **Processes** view. View and edit service process properties on each assigned node.
- **Connections and Locks** view. View and terminate repository connections and object locks.
- **Plug-ins** view. View and manage registered plug-ins.
- **Permissions** view. View or edit group and user permissions on the PowerCenter Repository Service.
- **Actions** menu. Manage the contents of the repository and perform other administrative tasks.

PowerExchange Listener Service

Runs the PowerExchange Listener.

When you select a Listener Service in the Navigator, the contents panel displays the following information:

- Service and service process status. Status of the service and service process for each node. The contents panel also displays the URL of the PowerExchange Listener instance.
- **Properties** view. View or edit Listener Service properties.
- **Actions** menu. Contains actions that you can perform on the Listener Service, such as viewing logs or enabling and disabling the service.

PowerExchange Logger Service

Runs the PowerExchange Logger for Linux, UNIX, and Windows.

When you select a Logger Service in the Navigator, the contents panel displays the following information:

- Service and service process status. Status of the service and service process for each node. The contents panel also displays the URL of the PowerExchange Logger instance.
- **Properties** view. View or edit Logger Service properties.

- **Actions** menu. Contains actions that you can perform on the Logger Service, such as viewing logs or enabling and disabling the service.

Reporting Service

Runs the Data Analyzer application in an Informatica domain. You log in to Data Analyzer to create and run reports on data in a relational database or to run the following PowerCenter reports: PowerCenter Repository Reports, Data Profiling Reports, or Metadata Manager Reports. You can also run other reports within your organization.

When you select a Reporting Service in the Navigator, the contents panel displays the following information:

- Service and service process status. Status of the service and service process for each node. The contents panel also displays the URL of the Data Analyzer instance.
- **Properties** view. The Reporting Service properties such as the data source properties or the Data Analyzer repository properties. You can edit some of these properties.
- **Permissions** view. View or edit group and user permissions on the Reporting Service.
- **Actions** menu. Manage the service and repository contents.

Reporting and Dashboards Service

Runs reports from the JasperReports application.

SAP BW Service

Listens for RFC requests from SAP BW and initiates workflows to extract from or load to SAP BW. Select an SAP BW Service in the Navigator to access properties and other information about the service.

When you select an SAP BW Service in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process.
- **Properties** view. Manage general properties and node assignments.
- **Associated Integration Service** view. View or edit the Integration Service associated with the SAP BW Service.
- **Processes** view. View or edit the directory of the BWParam parameter file.
- **Permissions** view. View or edit group and user permissions on the SAP BW Service.
- **Actions** menu. Manage the service.

Web Services Hub

A web service gateway for external clients. It processes SOAP requests from web service clients that want to access PowerCenter functionality through web services. Web service clients access the PowerCenter Integration Service and PowerCenter Repository Service through the Web Services Hub.

When you select a Web Services Hub in the Navigator, the contents panel displays the following information:

- Service and service process status. View the status of the service and the service process.
- **Properties** view. View or edit Web Services Hub properties.
- **Associated Repository** view. View the PowerCenter Repository Services associated with the Web Services Hub.
- **Permissions** view. View or edit group and user permissions on the Web Services Hub.
- **Actions** menu. Manage the service.

Nodes

A node is a logical representation of a physical machine in the domain. On the Domain tab, you assign resources to nodes and configure service processes to run on nodes.

When you select a node in the Navigator, the contents panel displays the following information:

- **Node status.** View the status of the node.
- **Properties** view. View or edit node properties, such as the repository backup directory or range of port numbers for the processes that run on the node.
- **Processes** view. View the status of processes configured to run on the node.
- **Resources** view. View or edit resources assigned to the node.
- **Permissions** view. View or edit group and user permissions on the node.

In the **Actions** menu in the Navigator, you can delete the node, move the node to a folder, refresh the contents on the **Domain** tab, or access help on the current tab.

In the **Actions** menu on the **Domain** tab, you can remove the node association, recalculate the CPU profile benchmark, or shut down the node.

Grids

A grid is an alias assigned to a group of nodes that run PowerCenter Integration Service or Data Integration Service jobs.

When you run a job on a grid, the Integration Service distributes the processing across multiple nodes in the grid. For example, when you run a profile on a grid, the Data Integration Service splits the work into multiple jobs and assigns each job to a node in the grid. You assign nodes to the grid in the **Services and Nodes** view on the **Domain** tab.

When you select a grid in the Navigator, the contents panel displays the following information:

- **Properties** view. View or edit node assignments to a grid.
- **Permissions** view. View or edit group and user permissions on the grid.

In the **Actions** menu in the Navigator, you can delete the grid, move the grid to a folder, refresh the contents on the **Domain** tab, or access help on the current tab.

Licenses

You create a license object on the **Domain** tab based on a license key file provided by Informatica.

After you create the license, you can assign services to the license.

When you select a license in the Navigator, the contents panel displays the following information:

- **Properties** view. View license properties, such as supported platforms, repositories, and licensed options. You can also edit the license description.
- **Assigned Services** view. View or edit the services assigned to the license.
- **Options** view. View the licensed PowerCenter options.
- **Permissions** view. View or edit user permissions on the license.

In the **Actions** menu in the Navigator, you can delete the license, move the license to a folder, refresh the contents on the **Domain** tab, or access help on the current tab.

In the **Actions** menu on the **Domain** tab, you can add an incremental key to a license.

Domain Tab - Connections View

The **Connections** view shows the domain and all connections in the domain.

The **Connections** view has the following components:

Navigator

Appears in the left pane of the **Domain** tab and displays the domain and the connections in the domain.

Contents panel

Appears in the right pane of the **Domain** tab and displays information about the domain or the connection that you select in the Navigator.

When you select the domain in the Navigator, the contents panel shows all connections in the domain. In the contents panel, you can filter or sort connections, or search for specific connections.

When you select a connection in the Navigator, the contents panel displays information about the connection and lets you complete tasks for the connection, depending on which of the following views you select:

- **Properties** view. View or edit connection properties.
- **Pooling** view. View or edit pooling properties for the connection.
- **Permissions** view. View or edit group or user permissions on the connection.

Also, the **Actions** menu lets you test a connection.

Actions menu in the Navigator

When you select the domain in the Navigator, you can create a connection.

When you select a connection in the Navigator, you can delete the connection.

Actions menu on the Domain tab

When you select a connection in the Navigator, you can edit direct permissions or assign permissions to the connection.

Logs Tab

The **Logs** tab shows logs.

On the **Logs** tab, you can view the following types of logs:

- Domain log. Domain log events are log events generated from the domain functions that the Service Manager performs.
- Service log. Service log events are log events generated by each application service.
- User Activity log. User Activity log events monitor user activity in the domain.

The **Logs** tab displays the following components for each type of log:

- Filter. Configure filter options for the logs.
- Log viewer. Displays log events based on the filter criteria.
- Reset filter. Reset the filter criteria.
- Copy rows. Copy the log text of the selected rows.

- **Actions** menu. Contains options to save, purge, and manage logs. It also contains filter options.

Reports Tab

The **Reports** tab shows domain reports.

On the **Reports** tab, you can run the following domain reports:

- License Management Report. Run a report to monitor the number of software options purchased for a license and the number of times a license exceeds usage limits. Run a report to monitor the usage of logical CPUs and PowerCenter Repository Services. You run the report for a license.
- Web Services Report. Run a report to analyze the performance of web services running on a Web Services Hub. You run the report for a time interval.

Monitoring Tab

On the **Monitoring** tab, you can monitor Data Integration Services and integration objects that run on the Data Integration Service.

Integration objects include jobs, applications, deployed mappings, logical data objects, SQL data services, web services, and workflows. The **Monitoring** tab displays properties, run-time statistics, and run-time reports about the integration objects.

The **Monitoring** tab contains the following components:

- Navigator. Appears in the left pane of the **Monitoring** tab and displays jobs, applications, and application components. Application components include deployed mappings, logical data objects, web services, and workflows.
- Contents panel. Appears in the right pane of the **Monitoring** tab. It contains information about the object that is selected in the Navigator.
 - If you select a folder in the Navigator, the contents panel lists all objects in the folder.
 - If you select an application component in the Navigator, multiple views of information about the object appear in the contents panel.
- Details panel. Appears below the contents panel in some cases. The details panel allows you to view details about the object that is selected in the contents panel.
- Actions menu. Appears on the **Monitoring** tab. Allows you to view context, reset search filters, abort a selected job, and view logs for a selected object.

Security Tab

You administer Informatica security on the Security tab of the Administrator tool.

The Security tab has the following components:

- Search section. Search for users, groups, or roles by name.

- Navigator. The Navigator appears in the left pane and displays groups, users, and roles.
- Contents panel. The contents panel displays properties and options based on the object selected in the Navigator and the tab selected in the contents panel.
- Security Actions menu. Contains options to create or delete a group, user, or role. You can manage LDAP and operating system profiles. You can also view users that have privileges for a service.

Using the Search Section

Use the Search section to search for users, groups, and roles by name. Search is not case sensitive.

1. In the Search section, select whether you want to search for users, groups, or roles.
2. Enter the name or partial name to search for.
You can include an asterisk (*) in a name to use a wildcard character in the search. For example, enter "ad*" to search for all objects starting with "ad". Enter "*ad" to search for all objects ending with "ad".
3. Click Go.
The Search Results section appears and displays a maximum of 100 objects. If your search returns more than 100 objects, narrow your search criteria to refine the search results.
4. Select an object in the Search Results section to display information about the object in the contents panel.

Using the Security Navigator

The Navigator appears in the contents panel of the Security tab. When you select an object in the Navigator, the contents panel displays information about the object.

The Navigator on the Security tab includes the following sections:

- Groups section. Select a group to view the properties of the group, the users assigned to the group, and the roles and privileges assigned to the group.
- Users section. Select a user to view the properties of the user, the groups the user belongs to, and the roles and privileges assigned to the user.
- Roles section. Select a role to view the properties of the role, the users and groups that have the role assigned to them, and the privileges assigned to the role.

The Navigator provides different ways to complete a task. You can use any of the following methods to manage groups, users, and roles:

- Click the Actions menu. Each section of the Navigator includes an Actions menu to manage groups, users, or roles. Select an object in the Navigator and click the Actions menu to create, delete, or move groups, users, or roles.
- Right-click an object. Right-click an object in the Navigator to display the create, delete, and move options available in the Actions menu.
- Drag an object from one section to another section. Select an object and drag it to another section of the Navigator to assign the object to another object. For example, to assign a user to a native group, you can select a user in the Users section of the Navigator and drag the user to a native group in the Groups section.
- Drag multiple users or roles from the contents panel to the Navigator. Select multiple users or roles in the contents panel and drag them to the Navigator to assign the objects to another object. For example, to assign multiple users to a native group, you can select the Native folder in the Users section of the Navigator to display all native users in the contents panel. Use the Ctrl or Shift keys to select multiple users and drag the selected users to a native group in the Groups section of the Navigator.

- Use keyboard shortcuts. Use keyboard shortcuts to move to different sections of the Navigator.

Groups

A group is a collection of users and groups that can have the same privileges, roles, and permissions.

The Groups section of the Navigator organizes groups into security domain folders. A security domain is a collection of user accounts and groups in an Informatica domain. Native authentication uses the Native security domain which contains the users and groups created and managed in the Administrator tool. LDAP authentication uses LDAP security domains which contain users and groups imported from the LDAP directory service.

When you select a security domain folder in the Groups section of the Navigator, the contents panel displays all groups belonging to the security domain. Right-click a group and select **Navigate to Item** to display the group details in the contents panel.

When you select a group in the Navigator, the contents panel displays the following tabs:

- **Overview.** Displays general properties of the group and users assigned to the group.
- **Privileges.** Displays the privileges and roles assigned to the group for the domain and for application services in the domain.

Users

A user with an account in the Informatica domain can log in to the following application clients:

- Informatica Administrator
- PowerCenter Client
- Metadata Manager
- Data Analyzer
- Informatica Developer
- Informatica Analyst
- Jaspersoft

The Users section of the Navigator organizes users into security domain folders. A security domain is a collection of user accounts and groups in an Informatica domain. Native authentication uses the Native security domain which contains the users and groups created and managed in the Administrator tool. LDAP authentication uses LDAP security domains which contain users and groups imported from the LDAP directory service.

When you select a security domain folder in the Users section of the Navigator, the contents panel displays all users belonging to the security domain. Right-click a user and select **Navigate to Item** to display the user details in the contents panel.

When you select a user in the Navigator, the contents panel displays the following tabs:

- **Overview.** Displays general properties of the user and all groups to which the user belongs.
- **Privileges.** Displays the privileges and roles assigned to the user for the domain and for application services in the domain.

Roles

A role is a collection of privileges that you assign to a user or group. Privileges determine the actions that users can perform. You assign a role to users and groups for the domain and for application services in the domain.

The Roles section of the Navigator organizes roles into the following folders:

- System-defined Roles. Contains roles that you cannot edit or delete. The Administrator role is a system-defined role.
- Custom Roles. Contains roles that you can create, edit, and delete. The Administrator tool includes some custom roles that you can edit and assign to users and groups.

When you select a folder in the Roles section of the Navigator, the contents panel displays all roles belonging to the folder. Right-click a role and select **Navigate to Item** to display the role details in the contents panel.




When you select a role in the Navigator, the contents panel displays the following tabs:

- Overview. Displays general properties of the role and the users and groups that have the role assigned for the domain and application services.
- Privileges. Displays the privileges assigned to the role for the domain and application services.

Service States

You can identify the state of the Informatica Services by the icon displayed in the Administrator tool.

The following table displays the icons associated with each service state:

State	Icon
Available	
Unavailable	
Disabled	






Process States

You can identify the state of a Data Integration Service process or PowerCenter Integration Service process by the icon displayed in the Administrator tool .

The icons for the state also depends the node in which the process runs. An yellow diamond overlay appears the process state icon if the primary node has high availability. A grid icon is superimposed the process state icon when the process runs a grid.

The following table displays the icons associated with the process states:










State	Icon
Aborted	
Aborted (with high availability)	
Aborted (Grid)	
Disabled	
Disabled (with high availability)	
Disabled (Grid)	
Failed	
Failed (with high availability)	
Failed (Grid)	
Running	
Running (with high availability)	
Running (Grid)	
Standing by or Delayed	
Standing by or Delayed (with high availability)	
Standing by or Delayed (Grid)	
Starting	
Starting (with high availability)	
Starting (Grid)	
Stopped	

State	Icon
Stopped (with high availability)	
Stopped (Grid)	
Stopping	
Stopping (with high availability)	
Stopping (Grid)	

Job States

You can identify the state of a job by the icon displayed in the Administrator tool.

The following table displays the icons associated with each job state:

State	Icon
Aborted	
Completed	
Failed	
In queue or Pending	
Running	
Starting	
Stopped	
Stopping	
Terminated	

Keyboard Shortcuts

You can use keyboard shortcuts to navigate and work with the Administrator tool interface.

You can add, edit, and change values in the Administrator tool. Keyboard focus in the Administrator tool is indicated by a blue border around the interface label. A dotted line appears around a selected object indicating that the object is in focus. Tooltips appear when the label item receives keyboard focus or on mouse-over.

Note: The navigation order of objects in the editor is from top to bottom and left to right.

You can perform the following tasks with keyboard shortcuts:

To navigate between different elements and select an element in the Administrator tool.

Press Tab.

Select the previous object.

Press Shift+Tab.

Navigate between perspective tabs.

Press the Left or Right arrow key to move between perspective tabs.

Select or clear check box and radio button.

Press the Space bar.

Upload files using the File Upload button.

Press the Space bar.

Navigate through records in a dialog box

Press the Up and Down arrow keys to navigate through different records.

Select and open drop-down menu item with sub-menus.

Press the Down arrow key. To go back to the main menu, press Esc.

Edit the value of grid content such as Access field and Revoke in Assign Permission and Edit permission dialog box.

Press the Space bar.

Note: You must enter appropriate values for all the form elements marked with an asterisk (*).

Move focus from Update Frequency drop-down menu to Time Range check box in the Statistics and Reports list grid in the Preferences dialog box of the Monitoring Tab or URL.

Press Esc.

You cannot access the Dependency Graph view or the Graphical Workflow view using the keyboard. You cannot access the split bars in the Administrator tool and increase or decrease the size of the panels using the keyboard. You cannot select multiple items with the Ctrl key in the Audit Reports tab under Security.

Note: To use the accessibility features in Internet Explorer 9 and 10, you must set the browser mode IE9 or IE10 Compatibility mode. To set the compatibility mode, press F12 and change the Browser Mode setting to match your version of Internet Explorer.

CHAPTER 4

Domain Management

This chapter includes the following topics:

- [Domain Management Overview, 46](#)
- [Alert Management, 47](#)
- [Folder Management, 49](#)
- [Domain Security Management, 50](#)
- [User Security Management, 51](#)
- [Application Service Management, 51](#)
- [Node Management, 54](#)
- [Gateway Configuration, 59](#)
- [Domain Configuration Management, 60](#)
- [Domain Tasks, 64](#)
- [Domain Properties, 67](#)

Domain Management Overview

An Informatica domain is a collection of nodes and services that define the Informatica environment. To manage the domain, you manage the nodes and services within the domain.

Use the Administrator tool to complete the following tasks:

- Manage alerts. Configure, enable, and disable domain and service alerts for users.
- Create folders. Create folders to organize domain objects and manage security by setting permission on folders.
- Manage domain security. Configure secure communication between domain components.
- Manage user security. Assign privileges and permissions to users and groups.
- Manage application services. Enable, disable, and remove application services. Enable, disable, and restart service processes.
- Manage nodes. Configure node properties, such as the backup directory and resources, and shut down nodes.
- Configure gateway nodes. Configure nodes to serve as a gateway.
- Shut down the domain. Shut down the domain to complete administrative tasks on the domain.

- Manage domain configuration. Back up the domain configuration on a regular basis. You might need to restore the domain configuration from a backup to migrate the configuration to another database user account. You might also need to reset the database information for the domain configuration if it changes.
- Complete domain tasks. You can monitor the statuses of all application services and nodes, view dependencies among application services and nodes, and shut down the domain.
- Configure domain properties. For example, you can change the database properties, SMTP properties for alerts, and domain resiliency properties.

To manage nodes and services through a single interface, all nodes and services must be in the same domain. You cannot access multiple Informatica domains in the same Administrator tool window. You can share metadata between domains when you register or unregister a local repository in the local Informatica domain with a global repository in another Informatica domain.

Alert Management

Alerts provide users with domain and service alerts. Domain alerts provide notification about node failure and master gateway election. Service alerts provide notification about service process failover.

To use the alerts, complete the following tasks:

- Configure the SMTP settings for the outgoing email server.
- Subscribe to alerts.

After you configure the SMTP settings, users can subscribe to domain and service alerts.

Configuring SMTP Settings

You configure the SMTP settings for the outgoing mail server to enable alerts.

Configure SMTP settings on the domain **Properties** view.

1. In the Administrator tool, click the **Domain** tab.
2. In the Navigator, select the domain.
3. In the contents panel, click the **Properties** view.
4. In the SMTP Configuration section, click **Edit**.
5. Edit the SMTP settings.

Property	Description
Host Name	The SMTP outbound mail server host name. For example, enter the Microsoft Exchange Server for Microsoft Outlook.
Port	Port used by the outgoing mail server. Valid values are from 1 to 65535. Default is 25.
User Name	The user name for authentication upon sending, if required by the outbound mail server.

Property	Description
Password	The user password for authentication upon sending, if required by the outbound mail server.
Sender Email Address	The email address that the Service Manager uses in the From field when sending notification emails. If you leave this field blank, the Service Manager uses Administrator@<host name> as the sender.

6. Click **OK**.

Subscribing to Alerts

After you complete the SMTP configuration, you can subscribe to alerts.

1. Verify that the domain administrator has entered a valid email address for your user account on the **Security** page.
If the email address or the SMTP configuration is not valid, the Service Manager cannot deliver the alert notification.
2. In the Administrator tool header area, click **Manage > Preferences**.
The **Preferences** page appears.
3. In the User Preferences section, click **Edit**.
The **Edit Preferences** dialog box appears.
4. Select **Subscribe for Alerts**.
5. Click **OK**.
6. Click **OK**.

The Service Manager sends alert notification emails based on your domain privileges and permissions.

The following table lists the alert types and events for notification emails:

Alert Type	Event
Domain	Node Failure Master Gateway Election
Service	Service Process Failover

Viewing Alerts

When you subscribe to alerts, you can receive domain and service notification emails for certain events. When a domain or service event occurs that triggers a notification, you can track the alert status in the following ways:

- The Service Manager sends an alert notification email to all subscribers with the appropriate privilege and permission on the domain or service.
- The Log Manager logs alert notification delivery success or failure in the domain or service log.

For example, the Service Manager sends the following notification email to all alert subscribers with the appropriate privilege and permission on the service that failed:

```
From: Administrator@<database host>
To: Jon Smith
Subject: Alert message of type [Service] for object [HR_811].
The service process on node [node01] for service [HR_811] terminated unexpectedly.
```

In addition, the Log Manager writes the following message to the service log:

```
ALERT_10009 Alert message [service process failover] of type [service] for object
[HR_811] was successfully sent.
```

You can review the domain or service logs for undeliverable alert notification emails. In the domain log, filter by Alerts as the category. In the service logs, search on the message code ALERT. When the Service Manager cannot send an alert notification email, the following message appears in the related domain or service log:

```
ALERT_10004: Unable to send alert of type [alert type] for object [object name], alert
message [alert message], with error [error].
```

Folder Management

Use folders in the domain to organize objects and to manage security. Folders can contain nodes, services, grids, licenses, and other folders. You might want to use folders to group services by type. For example, you can create a folder called IntegrationServices and move all Integration Services to the folder. Or, you might want to create folders to group all services for a functional area, such as Sales or Finance.

When you assign a user permission on the folder, the user inherits permission on all objects in the folder.

You can perform the following tasks with folders:

- View services and nodes. View all services in the folder and the nodes where they run. Click a node or service name to access the properties for that node or service.
- Create folders. Create folders to group objects in the domain.
- Move objects to folders. When you move an object to a folder, folder users inherit permission on the object in the folder. When you move a folder to another folder, the other folder becomes a parent of the moved folder.
- Remove folders. When you remove a folder, you can delete the objects in the folder or move them to the parent folder.

Creating a Folder

You can create a folder in the domain or in another folder.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the domain or folder in which you want to create a folder.
3. On the Navigator Actions menu, click New > Folder.

4. Edit the following properties:

Node Property	Description
Name	Name of the folder. The name is not case sensitive and must be unique within the domain. It cannot exceed 80 characters or begin with @. It also cannot contain spaces or the following special characters: <code>` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [</code>
Description	Description of the folder. The description cannot exceed 765 characters.
Path	Location in the Navigator.

5. Click OK.

Moving Objects to a Folder

When you move an object to a folder, folder users inherit permission on the object. When you move a folder to another folder, the moved folder becomes a child object of the folder where it resides.

Note: The domain serves as a folder when you move objects in and out of folders.

1. In the Informatica tool, click the Domain tab.
2. In the Navigator, select an object.
3. On the Navigator Actions menu, select Move to Folder.
4. In the Select Folder dialog box, select a folder, and click OK.

Removing a Folder

When you remove a folder, you can delete the objects in the folder or move them to the parent folder.

1. In the Informatica tool, click the Domain tab.
2. In the Navigator, select a folder.
3. On the Navigator Actions menu, select Delete.
4. Confirm that you want to delete the folder.

You can delete the contents only if you have the appropriate privileges and permissions on all objects in the folder.

5. Choose to wait until all processes complete or to abort all processes.
6. Click OK.

Domain Security Management

You can configure Informatica domain components to use the Secure Sockets Layer (SSL) protocol or the Transport Layer Security (TLS) protocol to encrypt connections with other components. When you enable SSL or TLS for domain components, you ensure secure communication.

You can configure secure communication in the following ways:

Between services within the domain

You can configure secure communication between services within the domain.

Between the domain and external components

You can configure secure communication between Informatica domain components and web browsers or web service clients.

Each method of configuring secure communication is independent of the other methods. When you configure secure communication for one set of components, you do not need to configure secure communication for any other set.

Note: If you change a secure domain to a non-secure domain or from a non-secure domain to a secure domain, you must delete the domain configuration in the Developer tool and PowerCenter client tools and configure the domain again in the client.

User Security Management

You manage user security within the domain with privileges and permissions.

Privileges determine the actions that users can complete on domain objects. Permissions define the level of access a user has to a domain object. Domain objects include the domain, folders, nodes, grids, licenses, database connections, operating system profiles, and application services.

Even if a user has the domain privilege to complete certain actions, the user might also require permission to complete the action on a particular object. For example, a user has the Manage Services domain privilege which grants the user the ability to edit application services. However, the user also must have permission on the application service. A user with the Manage Services domain privilege and permission on the Development Repository Service but not on the Production Repository Service can edit the Development Repository Service but not the Production Repository Service.

To log in to the Administrator tool, a user must have the Access Informatica Administrator domain privilege. If a user has the Access Informatica Administrator privilege and permission on an object, but does not have the domain privilege that grants the ability to modify the object type, then the user can view the object. For example, if a user has permission on a node, but does not have the Manage Nodes and Grids privilege, the user can view the node properties but cannot configure, shut down, or remove the node.

If a user does not have permission on a selected object in the Navigator, the contents panel displays a message indicating that permission on the object is denied.

Application Service Management

You can perform the following common administration tasks for application services:

- Enable and disable services and service processes.
- Configure the domain to restart service processes.
- Remove an application service.
- Troubleshoot problems with an application service.

Enabling and Disabling Services and Service Processes

You can enable and disable application services and service processes in the Administrator tool. When a service is enabled, there must be at least one service process enabled and running for the service to be available. By default, all service processes are enabled.

The behavior of a service when it starts service processes depends on its configuration:

- If the service is configured for high availability, the service starts the service process on the primary node. All backup nodes are on standby.
- If the service is configured to run on a grid, the service starts service processes on all nodes.

A service does not start a disabled service process in any situation.

The state of a service depends on the state of the constituent service processes. A service can have the following states:

- Available. You have enabled the service and at least one service process is running. The service is available to process requests.
- Unavailable. You have enabled the service but there are no service processes running. This can be a result of service processes being disabled or failing to start. The service is not available to process requests.
- Disabled. You have disabled the service.

You can disable a service to perform a management task, such as changing the data movement mode for a PowerCenter Integration Service. You might want to disable the service process on a node if you need to shut down the node for maintenance. When you disable a service, all associated service processes stop, but they remain enabled.

The following table describes the different states of a service process:

Service Process State	Process Configuration	Description
Running	Enabled	The service process is running on the node.
Standing By	Enabled	The service process is enabled but is not running because another service process is running as the primary service process. It is on standby to run in case of service failover. Note: Service processes cannot have a standby state when the PowerCenter Integration Service runs on a grid. If you run the PowerCenter Integration Service on a grid, all service processes run concurrently.
Disabled	Disabled	The service is enabled but the service process is stopped and is not running on the node.
Stopped	Enabled	The service is unavailable.
Failed	Enabled	The service and service process are enabled, but the service process could not start.

Note: A service process will be in a failed state if it cannot start on the assigned node.

Viewing Service Processes

You can view the state of a service process on the Processes view of a service. You can view the state of all service processes on the Overview view of the domain.

To view the state of a service process:

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select a service.
3. In the contents panel, select the Processes view.

The Processes view displays the state of the processes.

Configuring Restart for Service Processes

If an application service process becomes unavailable while a node is running, the domain tries to restart the process on the same node based on the restart options configured in the domain properties.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the domain.
3. In the Properties view, configure the following restart properties:

Domain Property	Description
Maximum Restart Attempts	Number of times within a specified period that the domain attempts to restart an application service process when it fails. The value must be greater than or equal to 1. Default is 3.
Within Restart Period (sec)	Maximum period of time that the domain spends attempting to restart an application service process when it fails. If a service fails to start after the specified number of attempts within this period of time, the service does not restart. Default is 900.

Removing Application Services

You can remove an application service using the Administrator tool. Before removing an application service, you must disable it.

Disable the service before you delete the service to ensure that the service is not running any processes. If you do not disable the service, you may have to choose to wait until all processes complete or abort all processes when you delete the service.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the application service.
3. In the Domain tab Actions menu, select Delete.
4. In the warning message that appears, click Yes to stop other services that depend on the application service.
5. If the Disable Service dialog box appears, choose to wait until all processes complete or abort all processes, and then click OK.

Troubleshooting Application Services

I think that a service is using incorrect environment variable values. How can I find out which environment variable values are used by a service.

Set the error severity level for the node to debug. When the service starts on the node, the Domain log will display the environment variables that the service is using.

Node Management

A node is a logical representation of a physical machine in the domain. During installation, you define at least one node that serves as the gateway for the domain. You can define other nodes using the installation program or *infasetup* command line program.

After you define a node, you must add the node to the domain. When you add a node to the domain, the node appears in the Navigator, and you can view and edit its properties. Use the Domain tab of Administrator tool to manage nodes, including configuring node properties and removing nodes from a domain.

You perform the following tasks to manage a node:

- Define the node and add it to the domain. Adds the node to the domain and enables the domain to communicate with the node. After you add a node to a domain, you can start the node.
- Configure properties. Configure node properties, such as the repository backup directory and ports used to run processes.
- View processes. View the processes configured to run on the node and their status. Before you remove or shut down a node, verify that all running processes are stopped.
- Shut down the node. Shut down the node if you need to perform maintenance on the machine or to ensure that domain configuration changes take effect.
- Remove a node. Remove a node from the domain if you no longer need the node.
- Define resources. When the PowerCenter Integration Service runs on a grid, you can configure it to check the resources available on each node. Assign connection resources and define custom and file/directory resources on a node.
- Edit permissions. View inherited permissions for the node and manage the object permissions for the node.

Note: If you add a node or remove a node, you must delete the domain configuration in the Developer tool and PowerCenter client tools and configure the domain again in the client.

Defining and Adding Nodes

You must define a node and add it to the domain so that you can start the node. When you install Informatica services, you define at least one node that serves as the gateway for the domain. You can define other nodes. The other nodes can be gateway nodes or worker nodes.

A master gateway node receives service requests from clients and routes them to the appropriate service and node. You can define one or more gateway nodes.

A worker node can run application services but cannot serve as a gateway.

When you define a node, you specify the host name and port number for the machine that hosts the node. You also specify the node name. The Administrator tool uses the node name to identify the node.

Use either of the following programs to define a node:

- Informatica installer. Run the installer on each machine you want to define as a node.
- *infasetup* command line program. Run the *infasetup* DefineGatewayNode or DefineWorkerNode command on each machine you want to serve as a gateway or worker node.

When you define a node, the installation program or *infasetup* creates the *nodemeta.xml* file, which is the node configuration file for the node. A gateway node uses information in the *nodemeta.xml* file to connect to the domain configuration database. A worker node uses the information in *nodemeta.xml* to connect to the domain. The *nodemeta.xml* file is stored in the *\isp\config* directory on each node.

After you define a node, you must add it to the domain. When you add a node to the domain, the node appears in the Navigator. You can add a node to the domain using the Administrator tool or the *infacmd* AddDomainNode command.

To add a node to the domain:

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the folder where you want to add the node. If you do not want the node to appear in a folder, select the domain.
3. On the Navigator Actions menu, click New > Node.
The Create Node dialog box appears.
4. Enter the node name. This must be the same node name you specified when you defined the node.
5. If you want to change the folder for the node, click Select Folder and choose a new folder or the domain.
6. Click Create.

If you add a node to the domain before you define the node using the installation program or *infasetup*, the Administrator tool displays a message saying that you need to run the installation program to associate the node with a physical host name and port number.

Configuring Node Properties

You configure node properties on the Properties view for the node. You can configure properties such as the error severity level and minimum and maximum port numbers.

1. In the Administrator tool, click the **Domain** tab.
2. In the Navigator, select a node.
3. Click the Properties view.
The Properties view displays the node properties in separate sections.
4. In the Properties view, click **Edit** for the section that contains the property you want to set.

5. Edit the following properties:

Node Property	Description
Name	Name of the node. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ()] [
Description	Description of the node. The description cannot exceed 765 characters.
Host Name	Host name of the machine represented by the node.
Port	Port number used by the node.
Gateway Node	Indicates whether the node can serve as a gateway. If this property is set to No , then the node is a worker node.
Backup Directory	Directory to store repository backup files. The directory must be accessible by the node.
Error Severity Level	Level of error logging for the node. These messages are written to the Log Manager application service and Service Manager log files. Set one of the following message levels: <ul style="list-style-type: none"> - ERROR. Writes ERROR code messages to the log. - WARNING. Writes WARNING and ERROR code messages to the log. - INFO. Writes INFO, WARNING, and ERROR code messages to the log. - TRACING. Writes TRACE, INFO, WARNING, and ERROR code messages to the log. - DEBUG. Writes DEBUG, TRACE, INFO, WARNING, and ERROR code messages to the log. Default is WARNING .
Minimum Port Number	Minimum port number used by service processes on the node. To apply changes, restart Informatica services. The default value is the value entered when the node was defined.
Maximum Port Number	Maximum port number used by service processes on the node. To apply changes, restart Informatica services. The default value is the value entered when the node was defined.
CPU Profile Benchmark	Ranks the node's CPU performance against a baseline system. For example, if the CPU is running 1.5 times as fast as the baseline machine, the value of this property is 1.5. You can calculate the benchmark by clicking Actions > Recalculate CPU Profile Benchmark . The calculation takes approximately five minutes and uses 100% of one CPU on the machine. Or, you can update the value manually. Default is 1.0. Minimum is 0.001. Maximum is 1,000,000. Used in adaptive dispatch mode. Ignored in round-robin and metric-based dispatch modes.

Node Property	Description
Maximum Processes	<p>Maximum number of running session tasks or command tasks allowed for each PowerCenter Integration Service process running on the node. For example, if you set the value to 5, up to 5 command tasks and 5 session tasks can run at the same time.</p> <p>Set this threshold to a high number, such as 200, to cause the Load Balancer to ignore it. To prevent the Load Balancer from dispatching tasks to this node, set this threshold to 0. Default is 10. Minimum is 0. Maximum is 1,000,000,000.</p> <p>Used in all dispatch modes.</p>
Maximum CPU Run Queue Length	<p>Maximum number of runnable threads waiting for CPU resources on the node. Set this threshold to a low number to preserve computing resources for other applications. Set this threshold to a high value, such as 200, to cause the Load Balancer to ignore it. Default is 10. Minimum is 0. Maximum is 1,000,000,000.</p> <p>Used in metric-based and adaptive dispatch modes. Ignored in round-robin dispatch mode.</p>
Maximum Memory %	<p>Maximum percentage of virtual memory allocated on the node relative to the total physical memory size.</p> <p>Set this threshold to a value greater than 100% to allow the allocation of virtual memory to exceed the physical memory size when dispatching tasks. Set this threshold to a high value, such as 1,000, if you want the Load Balancer to ignore it. Default is 150. Minimum is 0. Maximum is 1,000,000,000.</p> <p>Used in metric-based and adaptive dispatch modes. Ignored in round-robin dispatch mode.</p>
Log Collection Directory	<p>The directory that stores the logs for the application service when you run the log aggregator. The directory must be accessible from all the nodes in the domain. If the log collection directory is not accessible by other nodes, the aggregated logs do not appear in the aggregated logs listgrid. The users who run node processes must have read-write permissions on the directory.</p> <p>Configure the log collection directory for the master gateway node in the domain.</p>
Core Dump Directory	<p>The directory that stores the core dump files for the domain processes when you run the log aggregator.</p> <p>Configure the core dump directory for all the nodes in the domain.</p>

6. Click **OK**.

Viewing Processes on the Node

You can view the status of all processes configured to run on a node. Before you shut down or remove a node, you can view the status of each process to determine which processes you need to disable.

To view processes on a node:

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select a node.
3. In the content panel, select the Processes view.

The tab displays the status of each process configured to run on the node.

Shutting Down and Restarting the Node

Some administrative tasks may require you to shut down a node. For example, you might need to perform maintenance or benchmarking on a machine. You might also need to shut down and restart a node for some configuration changes to take effect. For example, if you change the shared directory for the Log Manager or domain, you must shut down the node and restart it to update the configuration files.

You can shut down a node from the Administrator tool or from the operating system. When you shut down a node, you stop Informatica services and abort all processes running on the node.

To restart a node, start Informatica services on the node.

Note: To avoid loss of data or metadata when you shut down a node, disable all running processes in complete mode.

Shutting Down a Node from the Administrator Tool

To shut down a node from the Administrator tool:

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select a node.
3. On the Domain tab Actions menu, select Shutdown.

The Administrator tool displays the list of service processes running on that node.

4. Click OK to stop all processes and shut down the node, or click Cancel to cancel the operation.

Starting or Stopping a Node on Windows

To start or stop the node on Windows:

1. Open the Windows Control Panel.
2. Select **Administrative Tools**.
3. Right-click **Services** and select **Run as Administrator**.
4. Right-click the Informatica service.
5. If the service is running, click **Stop**.
If the service is stopped, click **Start**.

Starting or Stopping a Node on UNIX

On UNIX, run `infaservice.sh` to start and stop the Informatica daemon. By default, `infaservice.sh` is installed in the following directory:

```
<InformaticaInstallationDir>/tomcat/bin
```

1. Go to the directory where `infaservice.sh` is located.
2. At the command prompt, enter the following command to start the daemon:

```
infaservice.sh startup
```

Enter the following command to stop the daemon:

```
infaservice.sh shutdown
```

Note: If you use a softlink to specify the location of `infaservice.sh`, set the `INFA_HOME` environment variable to the location of the Informatica installation directory.

Removing the Node Association

You can remove the host name and port number associated with a node. When you remove the node association, the node remains in the domain, but it is not associated with a host machine.

To associate a different host machine with the node, you must run the installation program or *infasetup* DefineGatewayNode or DefineWorkerNode command on the new host machine, and then restart the node on the new host machine.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select a node.
3. In the Domain tab Actions menu, select Remove Node Association.

Removing a Node

When you remove a node from a domain, it is no longer visible in the Navigator. If the node is running when you remove it, the node shuts down and all service processes are aborted.

Note: To avoid loss of data or metadata when you remove a node, disable all running processes in complete mode.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select a node.
3. In the Navigator Actions menu, select Delete.
4. In the warning message that appears, click OK.

Gateway Configuration

One gateway node in the domain serves as the master gateway node for the domain. The Service Manager on the master gateway node accepts service requests and manages the domain and services in the domain.

During installation, you create one gateway node. After installation, you can create additional gateway nodes. You might want to create additional gateway nodes as backups. If you have one gateway node and it becomes unavailable, the domain cannot accept service requests. If you have multiple gateway nodes and the master gateway node becomes unavailable, the Service Managers on the other gateway nodes elect a new master gateway node. The new master gateway node accepts service requests. Only one gateway node can be the master gateway node at any given time. You must have at least one node configured as a gateway node at all times. Otherwise, the domain is inoperable.

You can configure a worker node to serve as a gateway node with the *infasetup* SwitchGatewayNode command. The worker node must be running when you configure it to serve as a gateway node.

Note: You can also run the *infasetup* DefineGatewayNode command to create a gateway node. If you configure a worker node to serve as a gateway node, you must specify the log directory. If you have multiple gateway nodes, configure all gateway nodes to write log files to the same directory on a shared disk.

After you configure the gateway node, the Service Manager on the master gateway node writes the domain configuration database connection to the nodemeta.xml file of the new gateway node.

If you configure a master gateway node to serve as a worker node, you must restart the node to make the Service Managers elect a new master gateway node. If you do not restart the node, the node continues as the master gateway node until you restart the node or the node becomes unavailable.

1. In the Administrator tool, click the Domain tab.
2. In the Navigator, select the domain.
3. In the contents panel, select the Properties view.
4. In the Properties view, click Edit in the Gateway Configuration Properties section.
5. Select the check box next to the node that you want to serve as a gateway node.

You can select multiple nodes to serve as gateway nodes.

6. Configure the directory path for the log files.

If you have multiple gateway nodes, configure all gateway nodes to point to the same location for log files.

7. Click OK.

Domain Configuration Management

The Service Manager on the master gateway node manages the domain configuration. The domain configuration is a set of metadata tables stored in a relational database that is accessible by all gateway nodes in the domain. Each time you make a change to the domain, the Service Manager writes the change to the domain configuration. For example, when you add a node to the domain, the Service Manager adds the node information to the domain configuration. The gateway nodes use a JDBC connection to access the domain configuration database.

You can perform the following domain configuration management tasks:

- Back up the domain configuration. Back up the domain configuration on a regular basis. You may need to restore the domain configuration from a backup if the domain configuration in the database becomes corrupt.
- Restore the domain configuration. You may need to restore the domain configuration if you migrate the domain configuration to another database user account. Or, you may need to restore the backup domain configuration to a database user account.
- Migrate the domain configuration. You may need to migrate the domain configuration to another database user account.
- Configure the connection to the domain configuration database. Each gateway node must have access to the domain configuration database. You configure the database connection when you create a domain. If you change the database connection information or migrate the domain configuration to a new database, you must update the database connection information for each gateway node.
- Configure custom properties. Configure domain properties that are unique to your environment or that apply in special cases. Use custom properties only if Informatica Global Customer Support instructs you to do so.

Note: The domain configuration database and the Model repository cannot use the same database user schema.

Backing Up the Domain Configuration

Back up the domain configuration on a regular basis. You may need to restore the domain configuration from a backup file if the domain configuration in the database becomes corrupt.

Run the *infasetup* BackupDomain command to back up the domain configuration to a binary file.

Restoring the Domain Configuration

You can restore domain configuration from a backup file. You may need to restore the domain configuration if the domain configuration in the database becomes inconsistent or if you want to migrate the domain configuration to another database.

Informatica restores the domain configuration from the current version. If you have a backup file from an earlier product version, you must use the earlier version to restore the domain configuration.

You can restore the domain configuration to the same or a different database user account. If you restore the domain configuration to a database user account with existing domain configuration, you must configure the command to overwrite the existing domain configuration. If you do not configure the command to overwrite the existing domain configuration, the command fails.

Each node in a domain has a host name and port number. When you restore the domain configuration, you can disassociate the host names and port numbers for all nodes in the domain. You might do this if you want to run the nodes on different machines. After you restore the domain configuration, you can assign new host names and port numbers to the nodes. Run the *infasetup* DefineGatewayNode or DefineWorkerNode command to assign a new host name and port number to a node.

If you restore the domain configuration to another database, you must reset the database connections for all gateway nodes.

Important: You lose all data in the summary tables when you restore the domain configuration.

Complete the following tasks to restore the domain:

1. Disable the application services. Disable the application services in complete mode to ensure that you do not abort any running service process. You must disable the application services to ensure that no service process is running when you shut down the domain.
2. Shut down the domain. You must shut down the domain to ensure that no change to the domain occurs while you are restoring the domain.
3. Run the *infasetup* RestoreDomain command to restore the domain configuration to a database. The RestoreDomain command restores the domain configuration in the backup file to the specified database user account.
4. Assign new host names and port numbers to the nodes in the domain if you disassociated the previous host names and port numbers when you restored the domain configuration. Run the *infasetup* DefineGatewayNode or DefineWorkerNode command to assign a new host name and port number to a node.
5. Reset the database connections for all gateway nodes if you restored the domain configuration to another database. All gateway nodes must have a valid connection to the domain configuration database.

Migrating the Domain Configuration

You can migrate the domain configuration to another database user account. You may need to migrate the domain configuration if you no longer support the existing database user account. For example, if your

company requires all departments to migrate to a new database type, you must migrate the domain configuration.

1. Shut down all application services in the domain.
2. Shut down the domain.
3. Back up the domain configuration.
4. Create the database user account where you want to restore the domain configuration.
5. Restore the domain configuration backup to the database user account.
6. Update the database connection for each gateway node.
7. Start all nodes in the domain.
8. Enable all application services in the domain.

Important: Summary tables are lost when you restore the domain configuration.

Step 1. Shut Down All Application Services

You must disable all application services to disable all service processes. If you do not disable an application service and a user starts running a service process while you are backing up and restoring the domain, the service process changes may be lost and data may become corrupt.

Tip: Shut down the application services in complete mode to ensure that you do not abort any running service processes.

Shut down the application services in the following order:

1. Web Services Hub
2. SAP BW Service
3. Metadata Manager Service
4. PowerCenter Integration Service
5. PowerCenter Repository Service
6. Reporting Service
7. Search Service
8. Analyst Service
9. Content Management Service
10. Data Integration Service
11. Model Repository Service
12. Reporting and Dashboards Service

Step 2. Shut Down the Domain

You must shut down the domain to ensure that users do not modify the domain while you are migrating the domain configuration. For example, if the domain is running when you are backing up the domain configuration, users can create new services and objects. Also, if you do not shut down the domain and you restore the domain configuration to a different database, the domain becomes inoperative. The connections between the gateway nodes and the domain configuration database become invalid. The gateway nodes shut down because they cannot connect to the domain configuration database. A domain is inoperative if it has no running gateway node.

Step 3. Back Up the Domain Configuration

Run the *infasetup* BackupDomain command to back up the domain configuration to a binary file.

Step 4. Create a Database User Account

Create a database user account if you want to restore the domain configuration to a new database user account.

Step 5. Restore the Domain Configuration

Run the *infasetup* RestoreDomain command to restore the domain configuration to a database. The RestoreDomain command restores the domain configuration in the backup file to the specified database user account.

Step 6. Update the Database Connection

If you restore the domain configuration to a different database user account, you must update the database connection information for each gateway node in the domain. Gateway nodes must have a connection to the domain configuration database to retrieve and update domain configuration.

Step 7. Start All Nodes in the Domain

Start all nodes in the domain. You must start the nodes to enable services to run.

1. Shut down the gateway node that you want to update.
2. Run the *infasetup* UpdateGatewayNode command to update the gateway node.
3. Start the gateway node.
4. Repeat this process for each gateway node.

Step 8. Enable All Application Services

Enable all application services that you previously shut down. Application services must be enabled to run service processes.

Updating the Domain Configuration Database Connection

All gateway nodes must have a connection to the domain configuration database to retrieve and update domain configuration. When you create a gateway node or configure a node to serve as a gateway, you specify the database connection, including the database user name and password. If you migrate the domain configuration to a different database or change the database user name or password, you must update the database connection for each gateway node. For example, as part of a security policy, your company may require you to change the password for the domain configuration database every three months.

To update the node with the new database connection information, complete the following steps:

1. Shut down the gateway node.
2. Run the *infasetup* UpdateGatewayNode command.

If you change the user or password, you must update the node.

To update the node after you change the user or password, complete the following steps:

1. Shut down the gateway node.
2. Run the *infasetup* UpdateGatewayNode command.

If you change the host name or port number, you must redefine the node.

To redefine the node after you change the host name or port number, complete the following steps:

1. Shut down the gateway node.
2. In the Administrator tool, remove the node association.
3. Run the *infasetup* DefineGatewayNode command.

Domain Tasks

On the Domain tab, you can complete domain tasks such as monitoring application services and nodes, managing domain objects, managing logs, and viewing service and node dependencies.

You can monitor all application services and nodes in a domain. You can also manage domain objects by moving them into folders or deleting them. You can also recycle, enable, or disable application services and view logs for application services.

In addition, you can view dependencies among all application services and nodes. An application service is dependent on the node on which it runs. It might also be dependent on another application service. For example, the Data Integration Service must be associated with a Model Repository Service. If the Model Repository Service is unavailable, the Data Integration Service does not work.

To perform impact analysis, view dependencies among application services and nodes. Impact analysis helps you determine the implications of particular domain actions, such as shutting down a node or an application service. For example, you want to shut down a node to run maintenance on the node. Before you shut down the node, you must determine all application services that run on the node. If this is the only node on which an application service runs, that application service is unavailable when you shut down the node.

Managing and Monitoring Application Services and Nodes

You can manage and monitor application services and nodes in a domain.

1. In the Administrator tool, click the **Domain** tab.
2. Click the **Services and Nodes** view.
3. In the Navigator, select the domain.

The contents panel shows the objects defined in the domain.

4. To filter the list of domain objects in the contents panel, enter filter criteria in the filter bar.

The contents panel shows objects that meet the filter criteria.

5. To remove the filter criteria, click **Reset**.

The contents panel shows all objects defined in the domain.

6. To show the names of the application services and nodes in the contents panel, click the Show Details button.

The contents panel shows the names of the application services and nodes in the domain.

7. To hide the names of the application services and nodes in the contents panel, click the Hide Details button.

The contents panel hides the names of the application services and nodes in the domain.

8. To view details for an object, select the object in the Navigator.

For example, select an application service in the Navigator to view the service version, service status, process status, and last error message for the service.

Object details appear.

9. To view properties for an object, click an object in the Navigator.
The contents panels shows properties for the object.
10. To recycle, enable, disable, or show logs for an application service, double-click the application service in the Navigator.
 - To recycle the application service, click the Recycle the Service button.
 - To enable the application service, click the Enable the Service button.
 - To disable the application service, click the Disable the Service button.
 - To view logs for the application service, click the View Logs for Service button.
11. To move an object to a folder, complete the following steps:
 - a. Right-click the object in the Navigator.
 - b. Click **Move to Folder**.
The **Select Folder** dialog box appears.
 - c. In the **Select Folder** dialog box, select a folder.
Alternatively, to create a new folder, click **Create Folder**.
The **Create Folder** dialog box appears.
Enter the folder name and click **OK**.
 - d. Click **OK**.
The object is moved to the folder that you specify.
12. To delete an object, right-click the object in the Navigator.
Click **Delete**.

Viewing Dependencies for Application Services, Nodes, and Grids

In the Services and Nodes view on the Domain tab, you can view dependencies for application services, nodes, and grids in an Informatica domain.

To view the **View Dependency** window, you must install and enable Adobe Flash Player 10.0.0 or later in your browser. If you use Internet Explorer, enable the **Run ActiveX Controls and Plug-ins** option.

1. In the Administrator tool, click the **Domain** tab.
2. Click the **Services and Nodes** view.
3. In the Navigator, select the domain.
The contents panel displays the objects in the domain.
4. In the contents panel, right-click a domain object and click **View Dependencies**.
The **View Dependency** window shows domain objects connected by blue and orange lines, as follows:
 - The blue lines represent service-to-node and service-to-grid dependencies.
 - The orange lines represent service-to-service dependencies. To hide or show the service-to-service dependencies, clear or select the **Show Service dependencies** option in the **View Dependency** window. When you clear this option, the orange lines disappear but the services are still visible.

The following table describes the information that appears in the **View Dependency** window based on the object:

Object	View Dependency Window
Node	<p>Shows all service processes running on the node and the status of each process. Shows grids assigned to the node. Also shows secondary dependencies, which are dependencies that are not directly related to the object for which you are viewing dependencies.</p> <p>For example, a Model Repository Service, MRS1, runs on node1. A Data Integration Service, DIS1, and an Analyst Service, AT1, retrieve information from MRS1 but run on node2.</p> <p>The View Dependency window shows the following information:</p> <ul style="list-style-type: none"> - A dependency between node1 and MRS1. - A secondary dependency between node1 and the DIS1 and AT1 services. These services appear greyed out because they are secondary dependencies. <p>If you want to shut down node1, the window indicates that MRS1 is impacted, as well as DIS1 and AT1 due to their dependency on MRS1.</p>
Service	<p>Shows the upstream and downstream dependencies, and the node on which the service runs.</p> <p>An upstream dependency is a service on which the selected service depends. A downstream dependency is a service that depends on the selected service.</p> <p>For example, if you show the dependencies for a Data Integration Service, you see the Model Repository Service upstream dependency, the Analyst Service downstream dependency, and the node on which the Data Integration Service runs.</p>
Grid	Shows the nodes assigned to the grid and the application services running on the grid.

5. In the **View Dependency** window, you can optionally complete the following actions:
- To view additional dependency information for any object, place the cursor over the object.
 - To highlight the downstream dependencies and show additional process details for a service, place the cursor over the service.
 - To view the **View Dependency** window for any object in the window, right-click the object and click **Show Dependency**.
- The **View Dependency** window refreshes and shows the dependencies for the selected object.

Shutting Down a Domain

To run administrative tasks on a domain, you might need to shut down the domain.

For example, to back up and restore a domain configuration, you must first shut down the domain. When you shut down the domain, the Service Manager on the master gateway node stops all application services and Informatica services in the domain. After you shut down the domain, restart Informatica services on each node in the domain. On Windows, the Reporting Service process does not shut down when you shut down a domain. You must kill the Reporting Service process before you restart the nodes in a domain.

When you shut down a domain, any processes running on nodes in the domain are aborted. Before you shut down a domain, verify that all processes, including workflows, have completed and no users are logged in to repositories in the domain.

Note: To avoid a possible loss of data or metadata and allow the currently running processes to complete, you can shut down each node from the Administrator tool or from the operating system.

1. Click the **Domain** tab.
2. In the Navigator, select the domain.

3. On the **Domain** tab, click **Actions > Shutdown Domain**.
The **Shutdown** dialog box lists the processes that run in the domain.
4. Click **Yes**.
The **Shutdown** dialog box shows a warning message.
5. Click **Yes**.
The Service Manager on the master gateway node shuts down the application services and Informatica services on each node in the domain.
6. To restart the domain, restart Informatica services on the gateway and worker nodes in the domain.

Domain Properties

On the **Domain** tab, you can configure domain properties including database properties, gateway configuration, and service levels.

To view and edit properties, click the **Domain** tab. In the Navigator, select a domain. Then click the **Properties** view in the contents panel. The contents panel shows the properties for the domain.

You can configure the properties to change the domain. For example, you can change the database properties, SMTP properties for alerts, and the domain resiliency properties.

You can also monitor the domain at a high level. In the **Services and Nodes** view, you can view the statuses of the application services and nodes that are defined in the domain.

You can configure the following domain properties:

- General properties. Edit general properties, such as service resilience and dispatch mode.
- Database properties. View the database properties, such as database name and database host.
- Gateway configuration. Configure a node to serve as gateway and specify the location to write log events.
- Service level management. Create and configure service levels.
- SMTP configuration. Edit the SMTP settings for the outgoing mail server to enable alerts.
- Custom properties. Edit custom properties that are unique to the Informatica environment or that apply in special cases. When you create a domain, it has no custom properties. Use custom properties only at the request of Informatica Global Customer Support.

General Properties

In the General Properties area, you can configure general properties for the domain.

To edit general properties, click **Edit**.

The following table describes the properties that you can edit in the General Properties area:

Property	Description
Name	Read-only. The name of the domain.
Resilience Timeout	The number of seconds that an application service tries to connect or reconnect to the PowerCenter Repository Service or the PowerCenter Integration Service. Valid values are from 0 to 1000000. Default is 30 seconds.

Property	Description
Limit on Resilience Timeout	The maximum number of seconds that application clients or application services can try to connect or reconnect to the PowerCenter Repository Service or the PowerCenter Integration Service. Default is 180 seconds.
Restart Period	The maximum amount of time in seconds that the domain spends trying to restart an application service process. Valid values are from 0 to 1000000.
Maximum Restart Attempts within Restart Period	The number of times that the domain tries to restart an application service process. Valid values are from 0 to 1000. If you set the value as 0, the domain does not try to restart the service process.
Dispatch Mode	The mode that the Load Balancer uses to dispatch PowerCenter Integration Service tasks to nodes in a grid. Select one of the following dispatch modes: <ul style="list-style-type: none"> - MetricBased - RoundRobin - Adaptive
Enable Secure Communication	Configures services to use the TLS protocol to transfer data securely within the domain. When you enable secure communication for the domain, services use secure connections to communicate with other Informatica application services and clients. Verify that all domain nodes are available before you enable secure communication for the domain. If a node is not available, the secure communication changes cannot be applied to the Service Manager of the node. To apply changes, restart the domain. Set this property to True or False.
Service Resilience Timeout	The maximum number of seconds that application clients and application services can try to connect to the Data Integration Service or to the Model Repository Service. The default is 180 seconds.

Database Properties

In the Database Properties area, you can view or edit the database properties for the domain, such as database name and database host.

The following table describes the properties that you can edit in the Database Properties area:

Property	Description
Database Type	The type of database that stores the domain configuration metadata.
Database Host	The name of the machine hosting the database.
Database Port	The port number used by the database.
Database Name	The name of the database.
Database User	The user account for the database containing the domain configuration information.
Database TLS enabled	Indicates whether the database for the domain configuration repository is a secure database. True if the domain configuration repository database is secure. You can use a secure domain configuration repository if secure communication is enabled for the Informatica domain.

Note: The service manager uses the DataDirect drivers included with the Informatica installation. Informatica does not support the use of any other database driver.

Gateway Configuration Properties

In the Gateway Configuration Properties area, you can configure a node to serve as gateway for a domain and specify the directory where the Service Manager on this node writes the log event files.

If you edit gateway configuration properties, previous logs do not appear. Also, the changed properties apply to restart and failover scenarios only.

To edit gateway configuration properties, click **Edit**.

To sort gateway configuration properties, click the header of the column by which you want to sort.

The following table describes the properties that you can edit in the Gateway Configuration Properties area:

Property	Description
Node Name	Read-only. The name of the node.
Status	The status of the node.
Gateway	To configure the node as a gateway node, select this option. If the domain uses a secure domain configuration database, you must specify the truststore file and password for the database. To configure the node as a worker node, clear this option.
Log Directory Path	The directory path for the log event files. If the Log Manager cannot write to the directory path, it writes log events to the node.log file on the master gateway node.

Secure Domain Configuration Repository

If you configure a node as a gateway node and the domain uses a secure domain configuration database, you must specify the truststore file and password for the secure database.

If you configure multiple gateway nodes for the domain, set the database truststore file and password for all gateway nodes.

The following table describes the database truststore properties:

Property	Description
Database Truststore Password	Password for the truststore file.
Database Truststore Location	Path and file name of the truststore file for the secure database.

Note: To use a secure domain configuration repository database, the secure communication option must be enabled for the domain.

Service Level Management

In the Service Level Management area, you can view, add, and edit service levels.

Service levels set priorities among tasks that are waiting to be dispatched. When the Load Balancer has more tasks to dispatch than the PowerCenter Integration Service can run at the time, the Load Balancer places those tasks in the dispatch queue. When multiple tasks are in the dispatch queue, the Load Balancer uses service levels to determine the order in which to dispatch tasks from the queue.

Because service levels are domain properties, you can use the same service levels for all repositories in a domain. You create and edit service levels in the domain properties or by using `infacmd`.

You can edit but you cannot delete the Default service level, which has a dispatch priority of 5 and a maximum dispatch wait time of 1800 seconds.

To add a service level, click **Add**.

To edit a service level, click the link for the service level.

To delete a service level, select the service level and click the Delete button.

The following table describes the properties that you can edit in the Service Level Management area:

Property	Description
Name	The name of the service level. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with the @ character. It also cannot contain spaces or the following special characters: <code>` ~ % ^ * + = { } \ ; : / ? . < > ! ()] [</code> After you add a service level, you cannot change its name.
Dispatch Priority	A number that sets the dispatch priority for the service level. The Load Balancer dispatches high priority tasks before low priority tasks. Dispatch priority 1 is the highest priority. Valid values are from 1 to 10. Default is 5.
Maximum Dispatch Wait Time (seconds)	The amount of time in seconds that the Load Balancer waits before it changes the dispatch priority for a task to the highest priority. Setting this property ensures that no task waits forever in the dispatch queue. Valid values are from 1 to 86400. Default is 1800.

SMTP Configuration

In the SMTP Configuration area, you can configure SMTP settings for the outgoing mail server to enable alerts.

The following table describes the properties that you can edit in the SMTP Configuration area:

Property	Description
Host Name	The SMTP outbound mail server host name. For example, enter the Microsoft Exchange Server for Microsoft Outlook.
Port	Port used by the outgoing mail server. Valid values are from 1 to 65535. Default is 25.
User Name	The user name for authentication upon sending, if required by the outbound mail server.

Property	Description
Password	The user password for authentication upon sending, if required by the outbound mail server.
Sender Email Address	The email address that the Service Manager uses in the From field when sending notification emails. If you leave this field blank, the Service Manager uses <code>Administrator@<host name></code> as the sender.

Custom Properties for the Domain

Configure custom properties that are unique to specific environments.

You might need to apply custom properties in special cases. When you define a custom property, enter the property name and an initial value. Define custom properties only at the request of Informatica Global Customer Support.

CHAPTER 5

High Availability

This chapter includes the following topics:

- [High Availability Overview, 72](#)
- [Resilience, 73](#)
- [Restart and Failover, 75](#)
- [Recovery, 77](#)
- [Configuration for a Highly Available Domain, 77](#)
- [Troubleshooting High Availability, 81](#)

High Availability Overview

High availability refers to the uninterrupted availability of computer system resources. In an Informatica domain, high availability eliminates a single point of failure and provides minimal service interruption in the event of failure. When you configure high availability for a domain, the domain can continue running despite temporary network, hardware, or service failures.

The following high availability components make services highly available in an Informatica domain:

- **Resilience.** An Informatica domain can tolerate temporary connection failures until either the resilience timeout expires or the failure is fixed.
- **Restart and failover.** A process can restart on the same node or on a backup node after the process becomes unavailable.
- **Recovery.** Operations can complete after a service is interrupted. After a service process restarts or fails over, it restores the service state and recovers operations.

When you plan a highly available Informatica environment, configure high availability for both the internal Informatica components and systems that are external to Informatica. Internal components include the domain, application services, application clients, and command line programs. External systems include the network, hardware, database management systems, FTP servers, message queues, and shared storage.

High availability features for the Informatica environment are available based on your license.

Example

As you open a mapping in the PowerCenter Designer workspace, the PowerCenter Repository Service becomes unavailable and the request fails. The domain contains multiple nodes for failover and the PowerCenter Designer is resilient to temporary failures.

The PowerCenter Designer tries to establish a connection to the PowerCenter Repository Service within the resilience timeout period. The PowerCenter Repository Service fails over to another node because it cannot restart on the same node.

The PowerCenter Repository Service restarts within the resilience timeout period, and the PowerCenter Designer reestablishes the connection.

After the PowerCenter Designer reestablishes the connection, the PowerCenter Repository Service recovers from the failed operation and fetches the mapping into the PowerCenter Designer workspace.

Resilience

The domain tolerates temporary connection failures between application clients, application services, and nodes.

A temporary connection failure might occur because an application service process fails or because of a network failure. When a temporary connection failure occurs, the Service Manager tries to reestablish connections between the application clients, application services, and nodes.

Application Client Resilience

The application clients try to reconnect to application services when a temporary connection failure occurs.

Based on your license, the following application clients are resilient to the services that they connect to:

PowerCenter Client

The PowerCenter Client tries to reconnect to the PowerCenter Repository Service and the PowerCenter Integration Service when a temporary network failure occurs.

If you perform a PowerCenter Client action that requires connection to the repository while the PowerCenter Client is trying to reestablish the connection, the PowerCenter Client prompts you to try the operation again after the PowerCenter Client reestablishes the connection. If the PowerCenter Client is unable to reestablish the connection during the resilience timeout period, the PowerCenter Client prompts you to reconnect to the repository manually.

Command line programs

Command line programs try to reconnect to the domain or an application service when a temporary network failure occurs while a command line program is running.

Example PowerCenter Client Resilience to Application Services

There is a network connection loss of 120 seconds between the PowerCenter Workflow Monitor and the PowerCenter Repository Service when a developer is monitoring a workflow. The PowerCenter client, Workflow Monitor has a 60 second resilience timeout and the PowerCenter Repository Service has a resilience timeout of 180 seconds.

The Developer does not notice the loss of connection and he is unaffected by the 120 seconds connection loss. However, the following messages appear in the **Notifications** tab on the PowerCenter Workflow Monitor:

```
Repository Service notifications are enabled.  
DATE TIME-[REP_55101] Connection to the Repository Service [Repository_Service_Name] is  
broken.  
DATE TIME-[REP_55114] Reconnecting to the Repository Service [Repository_Service_Name].  
The resilience time is 180 seconds.  
DATE TIME-Reconnected to Repository Service [Repository_Service_Name] successfully.
```

Application Service Resilience

Some application services try to reconnect to application services, application clients, and external components when a temporary connection failure occurs.

Based on your license, the following application services are resilient to the temporary connection failure of their clients:

PowerCenter Integration Service

The PowerCenter Integration Service is resilient to temporary connection failures to other services, the PowerCenter client, and external components such as databases and FTP servers.

PowerCenter Repository Service

The PowerCenter Repository Service is resilient to temporary connection failures to other services, such as the PowerCenter Integration Service. It is also resilient to the temporary connection failures to the repository database.

Node Resilience

You can configure multiple nodes in a domain. Every node in the domain sends a communication signal to the master gateway node. The master gateway node is resilient to temporary failures in communication from the nodes in the domain.

Every node in the domain sends a communication signal to the master gateway node at periodic intervals of 15 seconds. The communication includes a list of services running on the node.

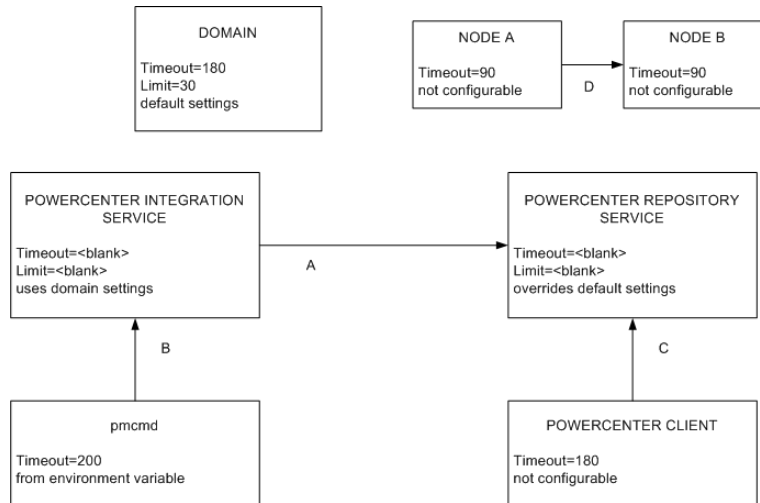
The master gateway node has resilience timeout of 90 seconds. If a node fails to connect to the master gateway node within the resilience timeout period, the master gateway node marks the node unavailable and reassigns its services to a backup node. This ensures that services on a node continue to run despite node failures.

Example Resilience Timeout Configuration

Some resilience timeout values are default and others can be configured or overwritten.

You can use the resilience timeout and limit on resilience timeout configured for the domain for PowerCenter application services if you do not set it for the application service. Command line programs use the service resilience timeout. If the service limit on resilience timeout is smaller than the resilience timeout for the connecting client, the client uses the services limit as the resilience timeout.

The following figure shows some sample connections and resilience configurations in a domain with PowerCenter application services:



The following table describes the resilience timeout and the limits shown in the figure above:

	Connect From	Connect To	Description
A	PowerCenter Integration Service	PowerCenter Repository Service	The PowerCenter Integration Service can spend up to 30 seconds to connect to the PowerCenter Repository Service, based on the domain resilience timeout. It is not bound by the PowerCenter Repository Service limit on resilience timeout of 60 seconds.
B	<i>pmcmd</i>	PowerCenter Integration Service	<i>pmcmd</i> is bound by the PowerCenter Integration Service limit on resilience timeout of 180 seconds, and it cannot use the 200 second resilience timeout configured in INFA_CLIENT_RESILIENCE_TIMEOUT.
C	PowerCenter Client	PowerCenter Repository Service	The PowerCenter Client is bound by the PowerCenter Repository Service limit on resilience timeout of 60 seconds. It cannot use the default resilience timeout of 180 seconds.
D	Node A	Node B	Node A can spend up to 90 seconds to connect to Node B. The Service Managers on Node A and Node B use the default node resilience timeout of 90 seconds.

Restart and Failover

To maximize operation time in the event of a failure, the Informatica domain can restart or fail over processes to another node.

The Service Manager on the master gateway node accepts application service request and manages the domain. If a master gateway node is not available, the domain shuts down. Configure the domain to failover to another node by configuring multiple gateway nodes.

Based on your license, you can also configure backup nodes for application services. The Service Manager can restart or failover the following application services if a failure occurs:

- Data Integration Service
- Model Repository Service
- PowerCenter Integration Service
- PowerCenter Repository Service
- PowerExchange Listener Service
- PowerExchange Logger Service

Domain Failover

The Service Manager on the master gateway node accepts service requests and manages the domain and services in the domain. The domain can failover to another node when the domain has multiple gateway nodes. Configure multiple gateway nodes to prevent domain shutdown when the master gateway node is unavailable.

The master gateway node maintains a connection to the domain configuration repository. If the domain configuration repository becomes unavailable, the master gateway node tries to reconnect when a user performs an operation. If the master gateway node cannot connect to the domain configuration repository, the master gateway node may shut down.

If the domain has multiple gateway nodes and the master gateway node becomes unavailable, the Service Managers on the other gateway nodes elect another master gateway node. The domain tries to connect to the domain configuration repository with each gateway node. If none of the gateway nodes can connect, the domain shuts down and all domain operations fail. When a master gateway fails over, the client tools retrieve information about the alternate domain gateways from the domains.infa file.

Note: Application services running on the master gateway node will not fail over when another master gateway node is elected unless the application service has a backup node configured.

Application Service Restart and Failover

If an application service process becomes unavailable, the Service Manager can restart the application service or fail it over to a backup node. When the Service Manager fails over an application service, it starts the service on another node that the service is configured to run on.

The following situations describe how the Service Manager restarts or fails over an application service:

- If the primary node running the service process becomes unavailable, the service fails over to a backup node. The primary node might be unavailable if it shuts down or if the connection to the node becomes unavailable.
- If the primary node running the service process is available, the domain tries to restart the process based on the restart options configured in the domain properties. If the process does not restart, the Service Manager may mark the process as failed. The service then fails over to a backup node and starts another process. If the Service Manager marks the process as failed, the administrator must enable the process after addressing any configuration problem.

If a service process fails over to a backup node, it does not fail back to the primary node when the node becomes available. You can disable the service process on the backup node to cause it to fail back to the primary node.

Recovery

Recovery is the completion of operations after an interrupted service is restored. The state of operation for a service contains information about the service process.

Based on your license, the following components can recover after an interrupted service is restored:

Service Manager

The Service Manager for each node in the domain maintains the state of service processes running on that node. If the master gateway shuts down, the newly elected master gateway collects the state information from each node to restore the state of the domain.

PowerCenter Repository Service

The PowerCenter Repository Service maintains the state of operation in the PowerCenter repository. The state of operation includes information about repository locks, requests in progress, and connected clients. After restart or failover, the PowerCenter Repository Service can recover operations from the point of interruption.

PowerCenter Integration Service

The PowerCenter Integration Service maintains the state of operation in the shared storage configured for the service. The state of operation includes information about scheduled, running, and completed tasks for the service.

The PowerCenter Integration Service maintains PowerCenter session and workflow state of operation based on the recovery strategy you configure for the session and workflow. When the PowerCenter Integration Service restarts or fails over a service process, it can automatically recover interrupted workflows that are configured for recovery.

Data Integration Service

The Data Integration Service maintains the state of operation in the Model repository. The state of operation includes the state of the workflow and workflow tasks and the values of the workflow variables and parameters during the interrupted workflow instance.

When a Data Integration Service process restarts or fails over a service process, you can manually restart interrupted workflows that are enabled for workflow recovery. You can also configure automatic recovery of aborted workflow instances due to an unexpected shutdown of the Data Integration Service process.

Configuration for a Highly Available Domain

To minimize system downtime, configure Informatica domain components to be highly available.

You can configure the following Informatica domain components to be highly available:

Domain

One node in the domain acts as a gateway to receive service requests from clients and routes them to the appropriate service and node. To prevent domain shutdown when the master gateway node is unavailable, configure more than one gateway node.

Nodes

Informatica services are processes that run on each node. You can configure Informatica services to restart automatically if it terminates unexpectedly.

Application Services

The application services run on nodes in the Informatica domain.

Based on your license, you can configure the following high availability features for application services:

- To minimize the application service downtime, configure backup nodes for application services.
- To specify the resilience period for application services, review default settings and configure resilience timeout periods for application services.
- To ensure PowerCenter Integration Service failover and recovery, configure the PowerCenter Integration Service to store process state information on a POSIX compliant shared file system or in a database.

Application Clients

Application clients provide access to Informatica functionality, and they run on user machines.

Application clients send requests to the Service Manager or application services.

You can configure resilience timeout periods for command line programs. You cannot configure a PowerCenter client resilience timeout.

External Systems

Use highly available versions of external systems such as source and target databases, message queues, and FTP servers.

Network

Make the network highly available by configuring redundant components such as routers, cables, and network adapters.

Application Service Resilience Configuration

When a temporary network failure occurs, application services try to reconnect to other application services for the duration of the resilience timeout. You can configure the resilience timeout for application services.

When an application service connects to another application service in the domain, the service that initiates the connection is a client of the other service.

You can configure application service resilience timeouts for the following application services:

PowerCenter Application Services

You can configure the resilience timeout and resilience timeout limits in the advanced properties of the PowerCenter Integration Service and PowerCenter Repository Service. The resilience timeout for application services that connects to a PowerCenter Integration Service or PowerCenter Repository Service is determined by one of the following values:

- The service **Resilience Timeout** property. You can configure the resilience timeout for the service in the service properties. To disable resilience for a service, set the resilience timeout to 0.
- The domain **Resilience Timeout** property. To use the resilience timeout configured for the domain, set the resilience timeout for the service to blank.
- The service **Limit on Resilience Timeout** property. If the service limit on resilience timeout is smaller than the resilience timeout for the connecting client, the client uses the limit as the resilience timeout. To use the limit on resilience timeout configured for the domain, set the service resilience limit to blank.
- The domain **Limit on Resilience Timeout** property. To use the resilience timeout configured for the domain, set the limit on resilience timeout for the service to blank.

You can configure the resilience timeout for the SAP BW Service in the general properties for the service. The SAP BW Service resilience timeout property is called the **Retry Period**.

Note: A client cannot be resilient to service interruptions if you disable the service in the Administrator tool. If you disable the service process, the client is resilient to the interruption in service.

Application Service Failover Configuration

Based on your license, you can configure backup nodes so that application services can failover to another node when the primary node fails. Configure backup nodes when you create or update an application service.

When you configure a backup node, verify that the node has access to run-time files that each application service requires to process data integration tasks such as workflows and mappings. For example, a workflow might require parameter files, input files, or output files.

PowerCenter Integration Service Failover and Recovery Configuration

During failover and recovery, the PowerCenter Integration Service needs access to information about which node was running the master PowerCenter Integration Service process and which node was running each session. You can configure the PowerCenter Integration Service to store process state information on a POSIX compliant shared file system or in a database.

Store High Availability Persistence on a POSIX Compliant Shared File System

By default, the PowerCenter Integration Service stores process state information in the \$PMStorageDir directory of the Integration Service process. Nodes that run the PowerCenter Integration Service must be on the same shared file system so that they can share resources. Also, nodes within a cluster must be on the cluster file system's heartbeat network.

Use a highly available POSIX compliant shared file system that is configured for I/O fencing. The hardware requirements and configuration of an I/O fencing solution are different for each file system.

The following shared file systems are certified by Informatica for use for PowerCenter Integration Service failover and session recovery:

Storage Array Network

- Veritas Cluster Files System (VxFS)

- IBM General Parallel File System (GPFS)

Network Attached Storage using NFS v3 protocol

- EMC UxFS hosted on an EMV Celerra NAS appliance

- NetApp WAFL hosted on a NetApp NAS appliance

Contact the file system vendors directly to evaluate which file system matches your requirements.

Store High Availability Persistence in a Database

The PowerCenter Integration Service can store process state information in database tables.

Configure the PowerCenter Integration Service to store process state in database tables in the advanced properties. The PowerCenter Integration Service stores process state information in persistent database tables in the associated PowerCenter repository database.

During failover, automatic recovery of workflows resume when the service process can access the database tables.

Command Line Program Resilience Configuration

You can configure the resilience timeout that command line programs use to perform domain and service operations.

When you use the `infacmd`, `pmcmd`, or `pmrep` command line programs to connect to the domain or an application service the resilience timeout is determined by the command line option, an environment variable, or the default resilience timeout.

Use the following guidelines when you configure command line program resilience:

Command line option

You can set the resilience timeout for `infacmd` by using the `-ResilienceTimeout` command line option each time you run a command. You can set the resilience timeout for `pmcmd` by using the `-timeout` command line option each time you run a command. When you use `pmrep` connect to connect to a repository, you can use the `-t` command line option to set the resilience timeout for `pmrep` commands that use the connection.

Environment variable.

If you do not set the timeout option in the `infacmd` and `pmcmd` command line syntax, the `infacmd` and `pmcmd` command line programs use the value of the environment variable `INFA_CLIENT_RESILIENCE_TIMEOUT` that is configured on the client machine. If you do not set the timeout option when you use `pmrep` connect to connect to the repository, `pmrep` commands use the value of the environment variable `INFA_CLIENT_RESILIENCE_TIMEOUT` that is configured on the client machine.

Default value

If you do not use the command line option or the environment variable, the `pmcmd` and `pmrep` command line program uses the default resilience timeout of 180 seconds. If you do not use the command line option or the environment variable, the `infacmd` command line program uses the value of the domain **Service Level Timeout** property as the default resilience timeout.

Limit on timeout

If the limit on resilience timeout for the PowerCenter Integration Service or the PowerCenter Repository Service is smaller than the command line resilience timeout, the command line program uses the limit as the resilience timeout.

Note: PowerCenter does not provide resilience for a repository client when the PowerCenter Repository Service is running in exclusive mode.

Domain Failover Configuration

You can define multiple gateway nodes to prevent domain shutdown when the master gateway node is unavailable.

During installation, you create one gateway node. After you install Informatica, you can define additional gateway nodes. To define a gateway node, add a gateway node to the domain or configure a worker node to serve as a gateway node.

Node Restart Configuration

The Informatica services runs the Service Manager on a node. You can configure the Informatica services to start automatically when a node terminates unexpectedly and restarts.

To restart the Informatica services when a node restarts, configure the following steps:

- In a UNIX environment, you can create a script to automatically start the Informatica services when the node starts.
- In a Windows environment, go to the Control Panel and configure the Informatica services to start automatically.

Troubleshooting High Availability

The solutions to the following situations might help you with high availability.

[I am not sure where to look for status information regarding client connections to the PowerCenter repository.](#)

In PowerCenter Client applications such as the PowerCenter Designer and the PowerCenter Workflow Manager, an error message appears if the connection cannot be established during the timeout period. Detailed information about the connection failure appears in the Output window. If you are using *pmrep*, the connection error information appears at the command line. If the PowerCenter Integration Service cannot establish a connection to the repository, the error appears in the PowerCenter Integration Service log, the workflow log, and the session log.

[I entered the wrong connection string for an Oracle database. Now I cannot enable the PowerCenter Repository Service even though I edited the PowerCenter Repository Service properties to use the right connection string.](#)

You need to wait for the database resilience timeout to expire before you can enable the PowerCenter Repository Service with the updated connection string.

[I have the high availability option, but my FTP server is not resilient when the network connection fails.](#)

The FTP server is an external system. To achieve high availability for FTP transmissions, you must use a highly available FTP server. For example, Microsoft IIS 6.0 does not natively support the restart of file uploads or file downloads. File restarts must be managed by the client connecting to the IIS server. If the transfer of a file to or from the IIS 6.0 server is interrupted and then reestablished within the client resilience timeout period, the transfer does not necessarily continue as expected. If the write process is more than half complete, the target file may be rejected.

[I have the high availability option, but the Informatica domain is not resilient when machines are connected through a network switch.](#)

If you are using a network switch to connect machines in the domain, use the auto-select option for the switch.

CHAPTER 6

Connections

This chapter includes the following topics:

- [Connections Overview, 82](#)
- [Connection Management, 82](#)
- [Pass-through Security, 85](#)
- [Pooling Properties in Connection Objects, 87](#)

Connections Overview

A connection is a repository object that defines a connection in the domain configuration repository.

The Data Integration Service uses database connections to process jobs for the Developer tool and the Analyst tool. Jobs include mappings, data profiles, scorecards, and SQL data services.

You can create and manage connections in the Administrator tool, the Developer tool, and the Analyst tool.

The tasks that you can perform in each tool depend on the tool that you use. For example, you can create an SAP NetWeaver connection in the Developer tool and manage it in the Administrator tool, but you cannot create or manage it in the Analyst tool.

Note: These connections are independent of the connections that you create in the PowerCenter Workflow Manager.

Connection Management

After you create a connection, you can view the connection, configure connection properties, and delete the connection.

After you create a connection, you can perform the following actions on the connection:

Configure connection pooling.

Configure connection pooling to optimize processing for the Data Integration Service. Connection pooling is a framework to cache connections.

View connection properties.

View the connection properties through the **Connections** view on the **Domain** tab.

Edit the connection.

You can change the connection name and the description. You can also edit connection details such as the user name, password, and connection strings. When you update a database connection that has connection pooling disabled, all updates take effect immediately.

The Data Integration Service identifies connections by the connection ID instead of the connection name. When you rename a connection, the Developer tool and the Analyst tool update the jobs that use the connection.

Deployed applications and parameter files identify a connection by name, not by connection ID. Therefore, when you rename a connection, you must redeploy all applications that use the connection. You must also update all parameter files that use the connection parameter.

Delete the connection.

When you delete a connection, objects that use the connection are no longer valid. If you accidentally delete a connection, you can re-create it by creating another connection with the same connection ID as the deleted connection.

Refresh the connections list.

You can refresh the connections list to see the latest list of connections for the domain. Refresh the connections list after a user adds, deletes, or renames a connection in the Developer tool or the Analyst tool.

Creating a Connection

In the Administrator tool, you can create relational database, social media, and file systems connections.

1. In the Administrator tool, click the **Domain** tab.
2. Click the **Connections** view.
3. In the Navigator, select the domain.
4. In the Navigator, click **Actions > New > Connection**.
The **New Connection** dialog box appears.
5. In the **New Connection** dialog box, select the connection type, and then click **OK**.
The **New Connection** wizard appears.
6. Enter the connection properties.
The connection properties that you enter depend on the connection type. Click **Next** to go to the next page of the **New Connection** wizard.
7. When you finish entering connection properties, you can click **Test Connection** to test the connection.
8. Click **Finish**.

Refreshing the Connections List

Refresh the connections list to see the latest list of connections in the domain.

The Administrator tool displays the latest list of connections when you start the Administrator tool. You might want to refresh the connections list when a user adds, deletes, or renames a connection in the Developer tool or the Analyst tool.

1. In the Administrator tool, click the **Domain** tab.
2. Click the **Connections** view.

The Navigator shows all connections in the domain.

3. In the Navigator, select the domain.
4. Click **Actions > Refresh**.

Viewing a Connection

View connections in the Administrator tool.

1. In the Administrator tool, click the **Domain** tab.
2. Click the **Connections** view.

The Navigator shows all connections in the domain.

3. In the Navigator, select the domain.

The contents panel shows all connections for the domain.

4. To filter the connections that appear in the contents panel, enter filter criteria and click the Filter button.

The contents panel shows the connections that meet the filter criteria.

5. To remove the filter criteria, click the Reset Filters button.

The contents panel shows all connections in the domain.

6. To sort the connections, click in the header for the column by which you want to sort the connections.

By default, connections are sorted by name.

7. To add or remove columns from the contents panel, right-click a column header.

If you have Read permission on the connection, you can view the data in the **Created By** column. Otherwise, this column is empty.

8. To view the connection details, select a connection in the Navigator.

The contents panel shows the connection details.

Configuring Pooling for a Connection

Configure pooling for a connection in the Administrator tool.

1. In the Administrator tool, click the **Domain** tab.
2. Click the **Connections** view.
3. In the Navigator, select a connection.

The contents panel shows the connection properties.

4. In the contents panel, click the **Pooling** view.
5. In the **Pooling Properties** area, click **Edit**.

The **Edit Pooling Properties** dialog box appears.

6. Edit the pooling properties and click **OK**.

Editing and Testing a Connection

In the Administrator tool, you can edit connections that you created in the Administrator tool, the Analyst tool, the Developer tool, or by running the `infacmd isp CreateConnection` command. You can test relational database connections.

1. In the Administrator tool, click the **Domain** tab.

2. Click the **Connections** view.

The Navigator shows all connections in the domain.

3. In the Navigator, select a connection.

The contents panel shows properties for the connection.

4. In the contents panel, select the **Properties** view or the **Pooling** view.

5. To edit properties in a section, click **Edit**.

Edit the properties and click **OK**.

Note: If you change a connection name, you must redeploy all applications that use the connection. You must also update all parameter files that use the connection parameter.

6. To test a database connection, select the connection in the Navigator.

Click **Actions > Test Connection** on the **Domain** tab.

A message box displays the result of the test.

Deleting a Connection

You can delete a database connection in the Administrator tool.

When you delete a connection in the Administrator tool, you also delete it from the Developer tool and the Analyst tool.

1. In the Administrator tool, click the **Domain** tab.

2. Click the **Connections** view.

The Navigator shows all connections in the domain.

3. In the Navigator, select a connection.

4. In the Navigator, click **Actions > Delete**.

Pass-through Security

Pass-through security is the capability to connect to an SQL data service or an external source with the client user credentials instead of the credentials from a connection object.

Users might have access to different sets of data based on the job in the organization. Client systems restrict access to databases by the user name and the password. When you create an SQL data service, you might combine data from different systems to create one view of the data. However, when you define the connection to the SQL data service, the connection has one user name and password.

If you configure pass-through security, you can restrict users from some of the data in an SQL data service based on their user name. When a user connects to the SQL data service, the Data Integration Service ignores the user name and the password in the connection object. The user connects with the client user name or the LDAP user name.

A web service operation mapping might need to use a connection object to access data. If you configure pass-through security and the web service uses WS-Security, the web service operation mapping connects to a source using the user name and password provided in the web service SOAP request.

Configure pass-through security for a connection in the connection properties of the Administrator tool or with `infacmd dis UpdateServiceOptions`. You can set pass-through security for connections to deployed

applications. You cannot set pass-through security in the Developer tool. Only SQL data services and web services recognize the pass-through security configuration.

For more information about configuring security for SQL data services, see the Informatica How-To Library article "How to Configure Security for SQL Data Services":
<http://communities.informatica.com/docs/DOC-4507>.

Example

An organization combines employee data from multiple databases to present a single view of employee data in an SQL data service. The SQL data service contains data from the Employee and Compensation databases. The Employee database contains name, address, and department information. The Compensation database contains salary and stock option information.

A user might have access to the Employee database but not the Compensation database. When the user runs a query against the SQL data service, the Data Integration Service replaces the credentials in each database connection with the user name and the user password. The query fails if the user includes salary information from the Compensation database.

Pass-Through Security with Data Object Caching

To use data object caching with pass-through security, you must enable caching in the pass-through security properties for the Data Integration Service.

When you deploy an SQL data service or a web service, you can choose to cache the logical data objects in a database. You must specify the database in which to store the data object cache. The Data Integration Service validates the user credentials for access to the cache database. If a user can connect to the cache database, the user has access to all tables in the cache. The Data Integration Service does not validate user credentials against the source databases when caching is enabled.

For example, you configure caching for the EmployeeSQLDS SQL data service and enable pass-through security for connections. The Data Integration Service caches tables from the Compensation and the Employee databases. A user might not have access to the Compensation database. However, if the user has access to the cache database, the user can select compensation data in an SQL query.

When you configure pass-through security, the default is to disallow data object caching for data objects that depend on pass-through connections. When you enable data object caching with pass-through security, verify that you do not allow unauthorized users access to some of the data in the cache. When you enable caching for pass-through security connections, you enable data object caching for all pass-through security connections.

Adding Pass-Through Security

Enable pass-through security for a connection in the connection properties. Enable data object caching for pass-through security connections in the pass-through security properties of the Data Integration Service.

1. Select a connection.
2. Click the **Properties** view.
3. Edit the connection properties.
The **Edit Connection Properties** dialog box appears.
4. To choose pass-through security for the connection, select the **Pass-through Security Enabled** option.
5. Optionally, select the Data Integration Service for which you want to enable object caching for pass-through security.
6. Click the **Properties** view.

7. Edit the pass-through security options.

The **Edit Pass-through Security Properties** dialog box appears.

8. Select **Allow Caching** to allow data object caching for the SQL data service or web service. This applies to all connections.
9. Click **OK**.

You must recycle the Data Integration Service to enable caching for the connections.

Pooling Properties in Connection Objects

You can edit connection pooling properties in the **Pooling** view for a database connection.

If the Data Integration Service runs jobs in separate operating system processes, the number of connection pool libraries depends on the number of running DTM processes. Each DTM process maintains its own connection pool library. The values of the pooling properties are for each connection pool library. For example, if you set maximum connections to 15, then each connection pool library can have a maximum of 15 idle connections in the pool. If you have three running DTM processes, then you can have a maximum of 45 idle connection instances.

To decrease the total number of idle connection instances, set the minimum number of connections to 0 and decrease the maximum idle time for each database connection.

The following list describes database connection pooling properties that you can edit in the **Pooling** view for a database connection:

Enable Connection Pooling

Enables connection pooling. When you enable connection pooling, each connection pool retains idle connection instances in memory. To delete the pools of idle connections, you must restart the Data Integration Service.

If connection pooling is disabled, the DTM process or the Data Integration Service process stops all pooling activity. The DTM process or the Data Integration Service process creates a connection instance each time it processes a job. It drops the instance when it finishes processing the job.

Default is enabled for DB2 for i5/OS, DB2 for z/OS, IBM DB2, Microsoft SQL Server, Oracle, and ODBC connections. Default is disabled for Adabas, IMS, Sequential, and VSAM connections.

Minimum # of Connections

The minimum number of idle connection instances that a pool maintains for a database connection after the maximum idle time is met. Set this value to be equal to or less than the maximum number of idle connection instances. Default is 0.

Maximum # of Connections

The maximum number of idle connection instances that a pool maintains for a database connection before the maximum idle time is met. Set this value to be more than the minimum number of idle connection instances. Default is 15.

Maximum Idle Time

The number of seconds that a connection instance that exceeds the minimum number of connection instances can remain idle before the connection pool drops it. The connection pool ignores the idle time when the connection instance does not exceed the minimum number of idle connection instances. Default is 120.

CHAPTER 7

Connection Properties

This chapter contains connection properties for each of the connections you can create and manage through Informatica clients.

Adabas Connection Properties

Use an Adabas connection to access an Adabas database. The Adabas connection is a mainframe database type connection. You create an Adabas connection in the Developer tool. You can manage an Adabas connection in the Administrator tool or the Developer tool.

The following table describes Adabas connection properties:

Option	Description
Location	Node name for the location of the PowerExchange Listener that connects to Adabas. The node name is defined in the first parameter of the NODE statement in the PowerExchange dbmover.cfg configuration file.
User Name	Database user name. For a database on a supported Linux or UNIX system, if you have enabled PowerExchange LDAP user authentication, the user name is the enterprise user name. For more information, see the <i>PowerExchange Reference Manual</i> .

Option	Description
Password	<p>Password for the database user name or a valid PowerExchange passphrase.</p> <p>A PowerExchange passphrase can be from 9 to 128 characters in length and can contain the following characters:</p> <ul style="list-style-type: none"> - Uppercase and lowercase letters - The numbers 0 to 9 - Spaces - The following special characters: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Note: The first character is an apostrophe.</p> <p>Passphrases cannot include single quotation marks ('), double quotation marks ("), or currency symbols.</p> <p>To use passphrases, ensure that the PowerExchange Listener runs with a security setting of SECURITY=(1,N) or higher in the DBMOVER member. For more information, see "SECURITY Statement" in the <i>PowerExchange Reference Manual</i>.</p> <p>The allowable characters in the IBM IRRPHREX exit do not affect the allowable characters in PowerExchange passphrases.</p> <p>Note: A valid RACF passphrase can be up to 100 characters in length. PowerExchange truncates passphrases longer than 100 characters when passing them to RACF for validation.</p>
Code Page	<p>Required. Name of the code page to use for reading from or writing to the data source. Usually, this value is an ISO code page name, such as ISO-8859-6.</p>
Pass-through security enabled	<p>Enables pass-through security for the connection. When you enable pass-through security for a connection, the domain uses the client user name and password to log into the corresponding database, instead of the credentials defined in the connection object.</p>
Encryption Type	<p>The type of encryption that the Data Integration Service uses. Select one of the following options:</p> <ul style="list-style-type: none"> - None - RC2 - DES <p>Default is None.</p> <p>Notes:</p> <ul style="list-style-type: none"> - Informatica recommends that you use Secure Sockets Layer (SSL) authentication instead of configuring the Encryption Type and Level connection properties or the ENCRYPT and ENCRYPTLEVEL statements in the DBMOVER configuration file. SSL authentication provides stricter security and is used by several Informatica products. <p>For more information about implementing SSL authentication in a PowerExchange network, see the <i>PowerExchange Reference Manual</i>.</p> <ul style="list-style-type: none"> - The values that you select for the Encryption Type and Level connection attributes override the values in the ENCRYPT and ENCRYPTLEVEL statements, if defined, in the DBMOVER configuration file on the Integration Service machine. To enable encryption for a mapping, be sure to select the appropriate connection attributes.
[Encryption] Level	<p>If you selected RC2 or DES for Encryption Type, select one of the following options to indicate the encryption level that the Data Integration Service uses:</p> <ul style="list-style-type: none"> - 1. Use a 56-bit encryption key for DES and RC2. - 2. Use 168-bit triple encryption key for DES, and use a 64-bit encryption key for RC2. - 3. Use 168-bit triple encryption key for DES, and use a 128-bit encryption key for RC2. <p>This option is ignored if you do not select an encryption type.</p> <p>Default is 1.</p>

Option	Description
Pacing size	Optional. Amount of data that the source system can pass to the PowerExchange Listener. Set the pacing size if an external application, database, or the Data Integration Service node is a bottleneck. User lower values for faster performance. The minimum value and default value is 0. A value of 0 provides the best performance.
Interpret as rows	Optional. Select this option to express the pacing size as a number of rows. Clear this option to express the pacing size in kilobytes. By default, this option is not selected and the pacing size is in kilobytes.
Compression	Optional. Select this option to enable source data compression. By compressing data, you can decrease the amount of data that Informatica applications send over the network. By default, this option is not selected and compression is disabled.
Offload processing	Optional. Controls whether to offload some bulk data processing from the source machine to the Data Integration Service machine. Select one of the following options: <ul style="list-style-type: none"> - AUTO. The Data Integration Service determines whether to use offload processing. - Yes. Use offload processing. - No. Do not use offload processing. Default is AUTO.
Worker threads	Optional. Number of threads that the Data Integration Service uses to process bulk data when offload processing is enabled. For optimal performance, this value should not exceed the number of available processors on the Data Integration Service machine. Valid values are 1 through 64. Default is 0, which disables multithreading.
Array size	Optional. The number of records in the storage array for the worker threads. This option is applicable when you set the Worker Threads option to a value greater than 0. Valid values are 1 to 100000. Default is 25.
Write mode	Optional. Mode in which Data Integration Service sends data to the PowerExchange Listener. Select one of the following write modes: <ul style="list-style-type: none"> - CONFIRMWRITEON. Sends data to the PowerExchange Listener and waits for a response before sending more data. Select this option when error recovery is a priority. However, this option might degrade performance. - CONFIRMWRITEOFF. Sends data to the PowerExchange Listener without waiting for a response. Use this option if you can reload the target table when an error occurs. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sends data to the PowerExchange Listener without waiting for a response. This option also enables error detection. This option combines the speed of CONFIRMWRITEOFF and the data integrity of CONFIRMWRITEON. Default is CONFIRMWRITEON.

DataSift Connection Properties

Use a DataSift connection to extract data from the DataSift streams. A DataSift connection is a social media connection. You can create and manage a DataSift connection in the Administrator tool or the Developer tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes DataSift connection properties:

Property	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	The description of the connection. The description cannot exceed 765 characters.
Location	The domain where you want to create the connection.
Type	The connection type. Select DataSift.
Username	User name for the DataSift account.
API Key	API key. The Developer API key is displayed in the Dashboard or Settings page in the DataSift account.

Facebook Connection Properties

Use a Facebook connection to access data from the Facebook web site. A Facebook connection is a social media connection. You can create and manage a Facebook connection in the Administrator tool or the Developer tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes Facebook connection properties:

Property	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	The description of the connection. The description cannot exceed 765 characters.
Location	The domain where you want to create the connection.
Type	The connection type. Select Facebook.

Property	Description
Do you have OAuth details?	Indicates whether you want to configure OAuth. Select one of the following values: <ul style="list-style-type: none"> - Yes. Indicates that you have the access token. - No. Launches the OAuth Utility.
Consumer Key	The App ID that you get when you create the application in Facebook. Facebook uses the key to identify the application.
Consumer Secret	The App Secret that you get when you create the application in Facebook. Facebook uses the secret to establish ownership of the consumer key.
Access Token	Access token that the OAuth Utility returns. Facebook uses this token instead of the user credentials to access the protected resources.
Access Secret	Access secret is not required for Facebook connection.
Scope	Permissions for the application. Enter the permissions you used to configure OAuth.

Greenplum Connection Properties

Use a Greenplum connection to connect to a Greenplum database. The Greenplum connection is a relational type connection. You can create and manage a Greenplum connection in the Administrator tool or the Developer tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

When you create a Greenplum connection, you enter information for metadata and data access.

The following table describes Greenplum connection properties:

Property	Description
Name	Name of the Greenplum relational connection.
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or fewer and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	Description of the connection. The description cannot exceed 765 characters.
Location	Domain on which you want to create the connection.
Type	Type of connection.

The user name, password, driver name, and connection string are required to import the metadata. The following table describes the properties for metadata access:

Property	Description
User Name	User name with permissions to access the Greenplum database.
Password	Password to connect to the Greenplum database.
Driver Name	The name of the Greenplum JDBC driver. For example: <code>com.pivotal.jdbc.GreenplumDriver</code> For more information about the driver, see the Greenplum documentation.
Connection String	Use the following connection URL: <code>jdbc:pivotal:greenplum:// <hostname>:<port>;DatabaseName=<database_name></code> For more information about the connection URL, see the Greenplum documentation.

PowerExchange for Greenplum uses the host name, port number, and database name to create a control file to provide load specifications to the Greenplum gpload bulk loading utility. It uses the Enable SSL option and the certificate path to establish secure communication to the Greenplum server over SSL.

The following table describes the connection properties for data access:

Property	Description
Host Name	Host name or IP address of the Greenplum server.
Port Number	Greenplum server port number. If you enter 0, the gpload utility reads from the environment variable \$PGPORT. Default is 5432.
Database Name	Name of the database.
Enable SSL	Select this option to establish secure communication between the gpload utility and the Greenplum server over SSL.
Certificate Path	Path where the SSL certificates for the Greenplum server are stored. For information about the files that need to be present in the certificates path, see the gpload documentation.

HBase Connection Properties

Use an HBase connection to access HBase. The HBase connection is a NoSQL connection. You can create and manage an HBase connection in the Administrator tool or the Developer tool. Hbase connection properties are case sensitive unless otherwise noted.

The following table describes HBase connection properties:

Property	Description
Name	The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * () - + = { [}] \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	The description of the connection. The description cannot exceed 4,000 characters.
Location	The domain where you want to create the connection.
Type	The connection type. Select HBase.
ZooKeeper Host(s)	Name of the machine that hosts the ZooKeeper server. The name is case sensitive. When the ZooKeeper runs in the replicated mode, specify a comma-separated list of servers in the ZooKeeper quorum servers. If the TCP connection to the server breaks, the client connects to a different server in the quorum.
ZooKeeper Port	Port number of the machine that hosts the ZooKeeper server.
Enable Kerberos Connection	Enables the Informatica domain to communicate with the HBase master server or region server that uses Kerberos authentication.

Property	Description
HBase Master Principal	<p>Service Principal Name (SPN) of the HBase master server. Enables the ZooKeeper server to communicate with an HBase master server that uses Kerberos authentication.</p> <p>Enter a string in the following format:</p> <pre>hbase/<domain.name>@<YOUR-REALM></pre> <p>Where:</p> <ul style="list-style-type: none"> - domain.name is the domain name of the machine that hosts the HBase master server. - YOUR-REALM is the Kerberos realm.
HBase Region Server Principal	<p>Service Principal Name (SPN) of the HBase region server. Enables the ZooKeeper server to communicate with an HBase region server that uses Kerberos authentication.</p> <p>Enter a string in the following format:</p> <pre>hbase_rs/<domain.name>@<YOUR-REALM></pre> <p>Where:</p> <ul style="list-style-type: none"> - domain.name is the domain name of the machine that hosts the HBase master server. - YOUR-REALM is the Kerberos realm.

HDFS Connection Properties

Use a Hadoop File System (HDFS) connection to access data in the Hadoop cluster. The HDFS connection is a file system type connection. You can create and manage an HDFS connection in the Administrator tool, Analyst tool, or the Developer tool. HDFS connection properties are case sensitive unless otherwise noted.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes HDFS connection properties:

Property	Description
Name	<p>Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:</p> <pre>~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /</pre>
ID	<p>String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.</p>
Description	<p>The description of the connection. The description cannot exceed 765 characters.</p>
Location	<p>The domain where you want to create the connection. Not valid for the Analyst tool.</p>
Type	<p>The connection type. Default is Hadoop File System.</p>

Property	Description
User Name	User name to access HDFS.
NameNode URI	<p>The URI to access HDFS.</p> <p>Use the following format to specify the NameNode URI in Cloudera and Hortonworks distributions:</p> <pre>hdfs://<namenode>:<port></pre> <p>Where</p> <ul style="list-style-type: none"> - <namenode> is the host name or IP address of the NameNode. - <port> is the port that the NameNode listens for remote procedure calls (RPC). <p>Use one of the following formats to specify the NameNode URI in MapR distribution:</p> <ul style="list-style-type: none"> - maprfs:/// - maprfs:///mapr/my.cluster.com/ <p>Where my.cluster.com is the cluster name that you specify in the mapr-clusters.conf file.</p>

Hive Connection Properties

Use the Hive connection to access Hive data. A Hive connection is a database type connection. You can create and manage a Hive connection in the Administrator tool, Analyst tool, or the Developer tool. Hive connection properties are case sensitive unless otherwise noted.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes Hive connection properties:

Property	Description
Name	<p>The name of the connection. The name is not case sensitive and must be unique within the domain. You can change this property after you create the connection. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:</p> <pre>~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /</pre>
ID	<p>String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.</p>
Description	<p>The description of the connection. The description cannot exceed 4000 characters.</p>
Location	<p>The domain where you want to create the connection. Not valid for the Analyst tool.</p>
Type	<p>The connection type. Select Hive.</p>

Property	Description
Connection Modes	<p>Hive connection mode. Select at least one of the following options:</p> <ul style="list-style-type: none"> - Access Hive as a source or target. Select this option if you want to use the connection to access the Hive data warehouse. If you want to use Hive as a target, you need to enable the same connection or another Hive connection to run mappings in the Hadoop cluster. - Use Hive to run mappings in Hadoop cluster. Select this option if you want to use the connection to run mappings in the Hadoop cluster. <p>You can select both the options. Default is Access Hive as a source or target.</p>
User Name	<p>User name of the user that the Data Integration Service impersonates to run mappings on a Hadoop cluster. The user name depends on the JDBC connection string that you specify in the Metadata Connection String or Data Access Connection String for the native environment.</p> <p>If the Hadoop cluster uses Kerberos authentication, the principal name for the JDBC connection string and the user name must match. Else, the user name depends on the behavior of the JDBC driver.</p> <p>If the Hadoop cluster does not use Kerberos authentication, the user name depends on the behavior of the JDBC driver.</p> <p>If you do not specify a user name, the Hadoop cluster authenticates jobs based on the following criteria:</p> <ul style="list-style-type: none"> - The Hadoop cluster does not use Kerberos authentication. It authenticates jobs based on the operating system profile user name of the machine that runs the Data Integration Service. - The Hadoop cluster uses Kerberos authentication. It authenticates jobs based on the SPN of the Data Integration Service.
Common Attributes to Both the Modes: Environment SQL	<p>SQL commands to set the Hadoop environment. In native environment type, the Data Integration Service executes the environment SQL each time it creates a connection to Hive metastore. If the Hive connection is used to run mappings in the Hadoop cluster, the Data Integration Service executes the environment SQL at the beginning of each Hive session.</p> <p>The following rules and guidelines apply to the usage of environment SQL in both the connection modes:</p> <ul style="list-style-type: none"> - Use the environment SQL to specify Hive queries. - Use the environment SQL to set the classpath for Hive user-defined functions and then use either environment SQL or PreSQL to specify the Hive user-defined functions. You cannot use PreSQL in the data object properties to specify the classpath. The path must be the fully qualified path to the JAR files used for user-defined functions. Set the parameter hive.aux.jars.path with all the entries in infapdo.aux.jars.path and the path to the JAR files for user-defined functions. - You can also use environment SQL to define Hadoop or Hive parameters that you intend to use in the PreSQL commands or in custom queries. <p>If the Hive connection is used to run mappings in the Hadoop cluster, only the environment SQL of the Hive connection is executed. The different environment SQL commands for the connections of the Hive source or target are not executed, even if the Hive sources and targets are on different clusters.</p>

Properties to Access Hive as Source or Target

The following table describes the connection properties that you configure to access Hive as a source or target:

Property	Description
Metadata Connection String	<p>The JDBC connection URI used to access the metadata from the Hadoop server.</p> <p>You can use PowerExchange for Hive to communicate with a HiveServer service or HiveServer2 service.</p> <p>To connect to HiveServer, specify the connection string in the following format: <code>jdbc:hive://<hostname>:<port>/<db></code></p> <p>Where</p> <ul style="list-style-type: none">- <code>hostname</code> is name or IP address of the machine on which HiveServer or HiveServer2 runs.- <code>port</code> is the port number on which HiveServer or HiveServer2 listens.- <code>db</code> is the database name to which you want to connect. If you do not provide the database name, the Data Integration Service uses the default database details. <p>To connect to HiveServer 2, use the connection string format that Apache Hive implements for that specific Hadoop Distribution. For more information about Apache Hive connection string formats, see the Apache Hive documentation.</p>
Bypass Hive JDBC Server	<p>JDBC driver mode. Select the checkbox to use the embedded JDBC driver (embedded mode).</p> <p>To use the JDBC embedded mode, perform the following tasks:</p> <ul style="list-style-type: none">- Verify that Hive client and Informatica Services are installed on the same machine.- Configure the Hive connection properties to run mappings in the Hadoop cluster. <p>If you choose the non-embedded mode, you must configure the Data Access Connection String. The JDBC embedded mode is preferred to the non-embedded mode.</p>
Data Access Connection String	<p>The connection string used to access data from the Hadoop data store.</p> <p>To connect to HiveServer, specify the non-embedded JDBC mode connection string in the following format: <code>jdbc:hive://<hostname>:<port>/<db></code></p> <p>Where</p> <ul style="list-style-type: none">- <code>hostname</code> is name or IP address of the machine on which HiveServer or HiveServer2 runs.- <code>port</code> is the port number on which HiveServer or HiveServer2 listens.- <code>db</code> is the database to which you want to connect. If you do not provide the database name, the Data Integration Service uses the default database details. <p>To connect to HiveServer 2, use the connection string format that Apache Hive implements for that specific Hadoop Distribution. For more information about Apache Hive connection string formats, see the Apache Hive documentation.</p>

Properties to Run Mappings in Hadoop Cluster

The following table describes the Hive connection properties that you configure when you want to use the Hive connection to run Informatica mappings in the Hadoop cluster:

Property	Description
Database Name	Namespace for tables. Use the name <code>default</code> for tables that do not have a specified database name.
Default FS URI	<p>The URI to access the default Hadoop Distributed File System.</p> <p>Use the following connection URI: <code>hdfs://<node name>:<port></code></p> <p>Where</p> <ul style="list-style-type: none">- <code>node name</code> is the host name or IP address of the NameNode.- <code>port</code> is the port on which the NameNode listens for remote procedure calls (RPC).
JobTracker/Yarn Resource Manager URI	<p>The service within Hadoop that submits the MapReduce tasks to specific nodes in the cluster.</p> <p>Use the following format: <code><hostname>:<port></code></p> <p>Where</p> <ul style="list-style-type: none">- <code>hostname</code> is the host name or IP address of the JobTracker or Yarn resource manager.- <code>port</code> is the port on which JobTracker or Yarn resource manager listens for remote procedure calls (RPC). <p>MapR distribution supports a highly available JobTracker. If you are using MapR distribution, define the JobTracker URI in the following format: <code>maprfs:///</code></p>
Hive Warehouse Directory on HDFS	<p>The absolute HDFS file path of the default database for the warehouse, which is local to the cluster. For example, the following file path specifies a local warehouse: <code>/user/hive/warehouse</code></p> <p>For Cloudera CDH, if the Metastore Execution Mode is remote, then the file path must match the file path specified by the Hive Metastore Service on the Hadoop cluster.</p>

Property	Description
Advanced Hive/Hadoop Properties	<p>Configures or overrides Hive or Hadoop cluster properties in hive-site.xml on the machine on which the Data Integration Service runs. You can specify multiple properties.</p> <p>Use the following format:</p> <pre><property1>=<value></pre> <p>Where</p> <ul style="list-style-type: none"> - <code>property1</code> is a Hive or Hadoop property in hive-site.xml. - <code>value</code> is the value of the Hive or Hadoop property. <p>To specify multiple properties use <code>&</code>: as the property separator.</p> <p>The maximum length for the format is 1 MB.</p> <p>If you enter a required property for a Hive connection, it overrides the property that you configure in the Advanced Hive/Hadoop Properties.</p> <p>The Data Integration Service adds or sets these properties for each map-reduce job. You can verify these properties in the JobConf of each mapper and reducer job. Access the JobConf of each job from the Jobtracker URL under each map-reduce job.</p> <p>The Data Integration Service writes messages for these properties to the Data Integration Service logs. The Data Integration Service must have the log tracing level set to log each row or have the log tracing level set to verbose initialization tracing.</p> <p>For example, specify the following properties to control and limit the number of reducers to run a mapping job:</p> <pre>mapred.reduce.tasks=2&hive.exec.reducers.max=10</pre>
Temporary Table Compression Codec	Hadoop compression library for a compression codec class name.
Codec Class Name	Codec class name that enables data compression and improves performance on temporary staging tables.
Metastore Execution Mode	Controls whether to connect to a remote metastore or a local metastore. By default, local is selected. For a local metastore, you must specify the Metastore Database URI, Driver, Username, and Password. For a remote metastore, you must specify only the Remote Metastore URI.
Metastore Database URI	<p>The JDBC connection URI used to access the data store in a local metastore setup. Use the following connection URI:</p> <pre>jdbc:<datastore type>://<node name>:<port>/<database name></pre> <p>where</p> <ul style="list-style-type: none"> - <code>node name</code> is the host name or IP address of the data store. - <code>data store type</code> is the type of the data store. - <code>port</code> is the port on which the data store listens for remote procedure calls (RPC). - <code>database name</code> is the name of the database. <p>For example, the following URI specifies a local metastore that uses MySQL as a data store:</p> <pre>jdbc:mysql://hostname23:3306/metastore</pre>
Metastore Database Driver	<p>Driver class name for the JDBC data store. For example, the following class name specifies a MySQL driver:</p> <pre>com.mysql.jdbc.Driver</pre>

Property	Description
Metastore Database Username	The metastore database user name.
Metastore Database Password	The password for the metastore user name.
Remote Metastore URI	<p>The metastore URI used to access metadata in a remote metastore setup. For a remote metastore, you must specify the Thrift server details.</p> <p>Use the following connection URI: <code>thrift://<hostname>:<port></code></p> <p>Where</p> <ul style="list-style-type: none"> - <code>hostname</code> is name or IP address of the Thrift metastore server. - <code>port</code> is the port on which the Thrift server is listening.

HTTP Connection Properties

Use an HTTP connection to connect a REST Web Service Consumer transformation to a web service. The HTTP connection is a web type connection. You create an HTTP connection in the Developer tool. You can manage an HTTP connection in the Administrator tool or the Developer tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes HTTP connection properties:

Property	Description
Name	<p>Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters:</p> <p>~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /</p>
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Username	<p>User name to connect to the web service. Enter a user name if you enable HTTP authentication or WS-Security.</p> <p>If the Web Service Consumer transformation includes WS-Security ports, the transformation receives a dynamic user name through an input port. The Data Integration Service overrides the user name defined in the connection.</p>
Password	<p>Password for the user name. Enter a password if you enable HTTP authentication or WS-Security.</p> <p>If the Web Service Consumer transformation includes WS-Security ports, the transformation receives a dynamic password through an input port. The Data Integration Service overrides the password defined in the connection.</p>
End Point URL	<p>URL for the web service that you want to access. The Data Integration Service overrides the URL defined in the WSDL file.</p> <p>If the Web Service Consumer transformation includes an endpoint URL port, the transformation dynamically receives the URL through an input port. The Data Integration Service overrides the URL defined in the connection.</p>

Property	Description
Timeout	Number of seconds that the Data Integration Service waits for a response from the web service provider before it closes the connection.
HTTP Authentication Type	Type of user authentication over HTTP. Select one of the following values: <ul style="list-style-type: none"> - None. No authentication. - Automatic. The Data Integration Service chooses the authentication type of the web service provider. - Basic. Requires you to provide a user name and password for the domain of the web service provider. The Data Integration Service sends the user name and the password to the web service provider for authentication. - Digest. Requires you to provide a user name and password for the domain of the web service provider. The Data Integration Service generates an encrypted message digest from the user name and password and sends it to the web service provider. The provider generates a temporary value for the user name and password and stores it in the Active Directory on the Domain Controller. It compares the value with the message digest. If they match, the web service provider authenticates you. - NTLM. Requires you to provide a domain name, server name, or default user name and password. The web service provider authenticates you based on the domain you are connected to. It gets the user name and password from the Windows Domain Controller and compares it with the user name and password that you provide. If they match, the web service provider authenticates you. NTLM authentication does not store encrypted passwords in the Active Directory on the Domain Controller.
Trust Certificates File	File containing the bundle of trusted certificates that the Data Integration Service uses when authenticating the SSL certificate of the web service. Enter the file name and full directory path. Default is <Informatica installation directory>/services/shared/bin/ca-bundle.crt.
Client Certificate File Name	Client certificate that a web service uses when authenticating a client. Specify the client certificate file if the web service needs to authenticate the Data Integration Service.
Client Certificate Password	Password for the client certificate. Specify the client certificate password if the web service needs to authenticate the Data Integration Service.
Client Certificate Type	Format of the client certificate file. Select one of the following values: <ul style="list-style-type: none"> - PEM. Files with the .pem extension. - DER. Files with the .cer or .der extension. Specify the client certificate type if the web service needs to authenticate the Data Integration Service.
Private Key File Name	Private key file for the client certificate. Specify the private key file if the web service needs to authenticate the Data Integration Service.
Private Key Password	Password for the private key of the client certificate. Specify the private key password if the web service needs to authenticate the Data Integration Service.
Private Key Type	Type of the private key. PEM is the supported type.

IBM DB2 Connection Properties

Use an IBM DB2 connection to access IBM DB2. An IBM DB2 connection is a relational database connection. You can create and manage an IBM DB2 connection in the Administrator tool, the Developer tool, or the Analyst tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes DB2 connection properties:

Property	Description
Database Type	The database type.
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	The description of the connection. The description cannot exceed 765 characters.
User Name	The database user name.
Password	The password for the database user name.
Pass-through security enabled	Enables pass-through security for the connection. When you enable pass-through security for a connection, the domain uses the client user name and password to log into the corresponding database, instead of the credentials defined in the connection object.
Connection String for data access	The DB2 connection URL used to access metadata from the database. dbname Where dbname is the alias configured in the DB2 client.
Metadata Access Properties: Connection String	Use the following connection URL: jdbc:informatica:db2://<host name>:<port>;DatabaseName=<database name>

Property	Description
AdvancedJDBCSecurityOptions	<p>Database parameters for metadata access to a secure database. Informatica treats the value of the AdvancedJDBCSecurityOptions field as sensitive data and stores the parameter string encrypted.</p> <p>To connect to a secure database, include the following parameters:</p> <ul style="list-style-type: none"> - EncryptionMethod. Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to SSL. - ValidateServerCertificate. Optional. Indicates whether Informatica validates the certificate that is sent by the database server. <p>If this parameter is set to True, Informatica validates the certificate that is sent by the database server. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate.</p> <p>If this parameter is set to false, Informatica does not validate the certificate that is sent by the database server. Informatica ignores any truststore information that you specify.</p> <ul style="list-style-type: none"> - HostNameInCertificate. Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate. - TrustStore. Required. Path and file name of the truststore file that contains the SSL certificate for the database. - TrustStorePassword. Required. Password for the truststore file for the secure database. <p>Note: Informatica appends the secure JDBC parameters to the connection string. If you include the secure JDBC parameters directly to the connection string, do not enter any parameters in the AdvancedJDBCSecurityOptions field.</p>
Data Access Properties: Connection String	<p>The connection string used to access data from the database.</p> <p>For IBM DB2 this is <database name></p>
Code Page	The code page used to read from a source database or to write to a target database or file.
Environment SQL	SQL commands to set the database environment when you connect to the database. The Data Integration Service runs the connection environment SQL each time it connects to the database.
Transaction SQL	SQL commands to set the database environment when you connect to the database. The Data Integration Service runs the transaction environment SQL at the beginning of each transaction.
Retry Period	This property is reserved for future use.
Tablespace	The tablespace name of the database.
SQL Identifier Character	<p>The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the Support Mixed-case Identifiers property.</p> <p>Select the character based on the database in the connection.</p>

Property	Description
Support Mixed-case Identifiers	When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. By default, this option is not selected.
ODBC Provider	ODBC. The type of database to which ODBC connects. For pushdown optimization, specify the database type to enable the Data Integration Service to generate native database SQL. The options are: <ul style="list-style-type: none"> - Other - Sybase - Microsoft_SQL_Server Default is Other.

IBM DB2 for i5/OS Connection Properties

Use an IBM DB2 for i5/OS connection to access tables in IBM DB2 for i5/OS. An IBM DB2 for i5/OS connection is a relational database connection. You can create and manage an IBM DB2 for i5/OS connection in the Administrator tool or the Developer tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes DB2 for i5/OS connection properties:

Property	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	The description of the connection. The description cannot exceed 255 characters.
Connection Type	The connection type (DB2I).
Username	A database user name.

Property	Description
Password	<p>A password for the specified user name or a valid PowerExchange passphrase.</p> <p>A PowerExchange passphrase can be from 9 to 31 characters in length and can contain the following characters:</p> <ul style="list-style-type: none"> - Uppercase and lowercase letters - The numbers 0 to 9 - Spaces - The following special characters: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Note: The first character is an apostrophe.</p> <p>Passphrases cannot include single quotation marks ('), double quotation marks ("), or currency symbols.</p> <p>To use passphrases, ensure that the PowerExchange Listener runs with a security setting of SECURITY=(1,N) or higher in the DBMOVER member. For more information, see "SECURITY Statement" in the <i>PowerExchange Reference Manual</i>.</p>
Pass-through security enabled	Enables pass-through security for the connection.
Database name	The database instance name.
Location	Node name for the location of the PowerExchange Listener that connects to DB2. The node name is defined in the first parameter of the NODE statement in the PowerExchange dbmover.cfg configuration file.
Environment SQL	SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database.
Database file overrides	<p>Specifies the i5/OS database file override in the following format:</p> <pre>from_file/to_library/to_file/to_member</pre> <p>Where:</p> <ul style="list-style-type: none"> - <i>from_file</i> is the file to be overridden. - <i>to_library</i> is the new library to use. - <i>to_file</i> is the file in the new library to use. - <i>to_member</i> is optional and is the member in the new library and file to use. *FIRST is used if nothing is specified. <p>You can specify up to eight unique file overrides on a single connection. A single override applies to a single source or target. When you specify more than one file override, enclose the string of file overrides in double quotes (") and include a space between each file override.</p> <p>Note: If you specify both Library List and Database File Overrides and a table exists in both, the Database File Overrides value takes precedence.</p>
Library list	<p>List of libraries that PowerExchange searches to qualify the table name for Select, Insert, Delete, or Update statements. PowerExchange searches the list if the table name is unqualified.</p> <p>Separate libraries with semicolons.</p> <p>Note: If you specify both Library List and Database File Overrides and a table exists in both, the Database File Overrides value takes precedence.</p>

Property	Description
Code Page	The code page used to read from a source database or write to a target database or file.
SQL Identifier character to use	The type of character used to identify special characters and reserved SQL keywords such as WHERE. The Data Integration Service places the identifier character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the Support mixed-case identifiers property.
Support mixed case identifiers	When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. By default, this option is not selected.
Isolation level	<p>Commit scope of the transaction. Select one of the following options:</p> <ul style="list-style-type: none"> - None - CS. Cursor stability. - RR. Repeatable Read. - CHG. Change. - ALL <p>Default is CS.</p>
Encryption type	<p>Optional. The type of encryption that the Data Integration Service uses. Select one of the following options:</p> <ul style="list-style-type: none"> - None - RC2 - DES <p>Default is None.</p> <p>Notes:</p> <ul style="list-style-type: none"> - Informatica recommends that you use Secure Sockets Layer (SSL) authentication instead of configuring the Encryption Type and Level connection properties or the ENCRYPT and ENCRYPTLEVEL statements in the DBMOVER configuration file. SSL authentication provides stricter security and is used by several Informatica products. <p>For more information about implementing SSL authentication in a PowerExchange network, see the <i>PowerExchange Reference Manual</i>.</p> <ul style="list-style-type: none"> - The values that you select for the Encryption Type and Level connection attributes override the values in the ENCRYPT and ENCRYPTLEVEL statements, if defined, in the DBMOVER configuration file on the Integration Service machine. To enable encryption for a mapping, be sure to select the appropriate connection attributes.
Encryption level	<p>If you selected RC2 or DES for Encryption Type, select one of the following options to indicate the encryption level that the Data Integration Service uses:</p> <ul style="list-style-type: none"> - 1. Use a 56-bit encryption key for DES and RC2. - 2. Use 168-bit triple encryption key for DES, and use a 64-bit encryption key for RC2. - 3. Use 168-bit triple encryption key for DES, and use a 128-bit encryption key for RC2. <p>This option is ignored if you do not select an encryption type.</p> <p>Default is 1.</p>
Pacing size	<p>Optional. Amount of data that the source system can pass to the PowerExchange Listener. Set the pacing size if an external application, database, or the Data Integration Service node is a bottleneck. User lower values for faster performance.</p> <p>The minimum value and default value is 0. A value of 0 provides the best performance.</p>

Property	Description
Interpret as rows	Optional. Select this option to express the pacing size as a number of rows. Clear this option to express the pacing size in kilobytes. By default, this option is not selected and the pacing size is in kilobytes.
Compression	Optional. Select this option to enable source data compression. By compressing data, you can decrease the amount of data that Informatica applications send over the network. By default, this option is not selected and compression is disabled.
Array size	Optional. The number of records in the storage array for the worker threads. This option is applicable when you set the Worker Threads option to a value greater than 0. Valid values are 25 to 100000. Default is 25.
Write mode	Optional. Mode in which the Data Integration Service sends data to the PowerExchange Listener. Select one of the following write modes: <ul style="list-style-type: none"> - CONFIRMWRITEON. Sends data to the PowerExchange Listener and waits for a response before sending more data. Select this option when error recovery is a priority. However, this option might degrade performance. - CONFIRMWRITEOFF. Sends data to the PowerExchange Listener without waiting for a response. Use this option if you can reload the target table when an error occurs. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sends data to the PowerExchange Listener without waiting for a response. This option also enables error detection. This option combines the speed of CONFIRMWRITEOFF and the data integrity of CONFIRMWRITEON. Default is CONFIRMWRITEON.
Reject file	Overrides the default prefix of PWXR for the reject file. PowerExchange creates the reject file on the target machine when the write mode is ASYNCHRONOUSWITHFAULTTOLERANCE. Enter PWXDISABLE to prevent the creation of the reject files.

IBM DB2 for z/OS Connection Properties

Use an IBM DB2 for z/OS connection to access tables in IBM DB2 for z/OS. An IBM DB2 for z/OS connection is a relational database connection. You can create and manage an IBM DB2 for z/OS connection in the Administrator tool or the Developer tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes DB2 for z/OS connection properties:

Property	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	Description of the connection. The description cannot exceed 255 characters.

Property	Description
Connection Type	Connection type (DB2Z).
Username	Database user name.
Password	<p>Password for the specified user name or a valid PowerExchange passphrase.</p> <p>A PowerExchange passphrase can be from 9 to 128 characters in length and can contain the following characters:</p> <ul style="list-style-type: none"> - Uppercase and lowercase letters - The numbers 0 to 9 - Spaces - The following special characters: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Note: The first character is an apostrophe.</p> <p>Passphrases cannot include single quotation marks ('), double quotation marks ("), or currency symbols.</p> <p>To use passphrases, ensure that the PowerExchange Listener runs with a security setting of SECURITY=(1,N) or higher in the DBMOVER member. For more information, see "SECURITY Statement" in the <i>PowerExchange Reference Manual</i>.</p> <p>The allowable characters in the IBM IRRPHREX exit do not affect the allowable characters in PowerExchange passphrases.</p> <p>Note: A valid RACF passphrase can be up to 100 characters in length. PowerExchange truncates passphrases longer than 100 characters when passing them to RACF for validation.</p>
Pass-through security enabled	Enables pass-through security for the connection.
DB2 Subsystem ID	Name of the DB2 subsystem.
Location	Node name for the location of the PowerExchange Listener that connects to DB2. The node name is defined in the first parameter of the NODE statement in the PowerExchange dbmover.cfg configuration file.
Environment SQL	SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database.
Correlation ID	Value to be concatenated to prefix PWX to form the DB2 correlation ID for DB2 requests.
Code Page	Code page used to read from a source database or write to a target database or file.
SQL identifier character to use	The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the Support mixed-case identifiers property.
Support mixed case identifiers	Select this option to have the Data Integration Service place identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Select this option when the objects have mixed-case or lowercase names. By default, this option is not selected.

Property	Description
Encryption type	<p>Optional. The type of encryption that the Data Integration Service uses. Select one of the following options:</p> <ul style="list-style-type: none"> - None - RC2 - DES <p>Default is None.</p> <p>Notes:</p> <ul style="list-style-type: none"> - Informatica recommends that you use Secure Sockets Layer (SSL) authentication instead of configuring the Encryption Type and Level connection properties or the ENCRYPT and ENCRYPTLEVEL statements in the DBMOVER configuration file. SSL authentication provides stricter security and is used by several Informatica products. <p>For more information about implementing SSL authentication in a PowerExchange network, see the <i>PowerExchange Reference Manual</i>.</p> <ul style="list-style-type: none"> - The values that you select for the Encryption Type and Level connection attributes override the values in the ENCRYPT and ENCRYPTLEVEL statements, if defined, in the DBMOVER configuration file on the Integration Service machine. To enable encryption for a mapping, be sure to select the appropriate connection attributes.
Encryption level	<p>If you selected RC2 or DES for Encryption Type, select one of the following options to indicate the encryption level that the Data Integration Service uses:</p> <ul style="list-style-type: none"> - 1. Use a 56-bit encryption key for DES and RC2. - 2. Use 168-bit triple encryption key for DES, and use a 64-bit encryption key for RC2. - 3. Use 168-bit triple encryption key for DES, and use a 128-bit encryption key for RC2. <p>This option is ignored if you do not select an encryption type.</p> <p>Default is 1.</p>
Pacing size	<p>Optional. Amount of data that the source system can pass to the PowerExchange Listener. Set the pacing size if an external application, database, or the Data Integration Service node is a bottleneck. User lower values for faster performance.</p> <p>The minimum value and default value is 0. A value of 0 provides the best performance.</p>
Interpret as rows	<p>Optional. Select this option to express the pacing size as a number of rows. Clear this option to express the pacing size in kilobytes. By default, this option is not selected and the pacing size is in kilobytes.</p>
Compression	<p>Optional. Select this option to enable source data compression. By compressing data, you can decrease the amount of data that Informatica applications send over the network. By default, this option is not selected and compression is disabled.</p>
Offload processing	<p>Optional. Controls whether to offload some bulk data processing from the source machine to the Data Integration Service machine. Select one of the following options:</p> <ul style="list-style-type: none"> - AUTO. The Data Integration Service determines whether to use offload processing. - Yes. Use offload processing. - No. Do not use offload processing. <p>Default is No.</p>
Worker threads	<p>Optional. Number of threads that the Data Integration Service uses to process bulk data when offload processing is enabled. For optimal performance, this value should not exceed the number of available processors on the Data Integration Service machine. Valid values are 1 through 64. Default is 0, which disables multithreading.</p>
Array size	<p>Optional. The number of records in the storage array for the worker threads. This option is applicable when you set the Worker Threads option to a value greater than 0. Valid values are 1 to 100000. Default is 25.</p>

Property	Description
Write mode	<p>Mode in which the Data Integration Service sends data to the PowerExchange Listener. Configure one of the following write modes:</p> <ul style="list-style-type: none"> - CONFIRMWRITEON. Sends data to the PowerExchange Listener and waits for a response before sending more data. Select if error recovery is a priority. This option might decrease performance. - CONFIRMWRITEOFF. Sends data to the PowerExchange Listener without waiting for a response. Use this option when you can reload the target table if an error occurs. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sends data to the PowerExchange Listener without waiting for a response. This option also provides the ability to detect errors. This provides the speed of Confirm Write Off with the data integrity of Confirm Write On. <p>Default is CONFIRMWRITEON.</p>
Reject file	<p>Overrides the default prefix of PWXR for the reject file. PowerExchange creates the reject file on the target machine when the write mode is ASYNCHRONOUSWITHFAULTTOLERANCE. Enter PWXDISABLE to prevent the creation of reject files.</p>

IMS Connection Properties

Use an IMS connection to access an IMS database. The IMS connection is a non-relational mainframe database type connection. The Data Integration Service connects to IMS through PowerExchange. You create an IMS connection in the Developer tool. You can manage an IMS connection in the Administrator tool or the Developer tool.

The following table describes IMS connection properties:

Option	Description
Location	Node name for the location of the PowerExchange Listener that connects to IMS. The node name is defined in the first parameter of the NODE statement in the PowerExchange dbmover.cfg configuration file.
User name	Database user name.

Option	Description
Password	<p>Password for the specified database user name or a valid PowerExchange passphrase. A PowerExchange passphrase can be from 9 to 128 characters in length and can contain the following characters:</p> <ul style="list-style-type: none"> - Uppercase and lowercase letters - The numbers 0 to 9 - Spaces - The following special characters: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Note: The first character is an apostrophe.</p> <p>Passphrases cannot include single quotation marks ('), double quotation marks ("), or currency symbols.</p> <p>The allowable characters in the IBM IRRPHREX exit do not affect the allowable characters in PowerExchange passphrases.</p> <p>Note: A valid RACF passphrase can be up to 100 characters in length. PowerExchange truncates passphrases longer than 100 characters when passing them to RACF for validation.</p> <p>To use passphrases for IMS connections, ensure that the following requirements are met:</p> <ul style="list-style-type: none"> - The PowerExchange Listener must run with a security setting of SECURITY=(1,N) or higher in the DBMOVER member. For more information, see "SECURITY Statement" in the <i>PowerExchange Reference Manual</i>. - You must configure ODBA access to IMS as described in the <i>PowerExchange Navigator User Guide</i>. - You must use IMS data maps that specify IMS ODBA as the access method. Do not use data maps that specify the DL/1 BATCH access method because this access method requires the use of netport jobs, which do not support passphrases. - The IMS database must be online in the IMS control region to use ODBA access to IMS.
Code page	<p>Required. Name of the code page to use for reading from or writing to the data source. Usually, this value is an ISO code page name, such as ISO-8859-6.</p>
Pass-through security enabled	<p>Enables pass-through security for the connection.</p>
Encryption type	<p>The type of encryption that the Data Integration Service uses. Select one of the following options:</p> <ul style="list-style-type: none"> - None - RC2 - DES <p>Default is None.</p> <p>Notes:</p> <ul style="list-style-type: none"> - Informatica recommends that you use Secure Sockets Layer (SSL) authentication instead of configuring the Encryption Type and Level connection properties or the ENCRYPT and ENCRYPTLEVEL statements in the DBMOVER configuration file. SSL authentication provides stricter security and is used by several Informatica products. <p>For more information about implementing SSL authentication in a PowerExchange network, see the <i>PowerExchange Reference Manual</i>.</p> <ul style="list-style-type: none"> - The values that you select for the Encryption Type and Level connection attributes override the values in the ENCRYPT and ENCRYPTLEVEL statements, if defined, in the DBMOVER configuration file on the Integration Service machine. To enable encryption for a mapping, be sure to select the appropriate connection attributes.

Option	Description
[Encryption] Level	<p>If you selected RC2 or DES for Encryption Type, select one of the following options to indicate the encryption level that the Data Integration Service uses:</p> <ul style="list-style-type: none"> - 1. Use a 56-bit encryption key for DES and RC2. - 2. Use 168-bit triple encryption key for DES, and use a 64-bit encryption key for RC2. - 3. Use 168-bit triple encryption key for DES, and use a 128-bit encryption key for RC2. <p>This option is ignored if you do not select an encryption type.</p> <p>Default is 1.</p>
Pacing size	<p>Optional. Amount of data that the source system can pass to the PowerExchange Listener. Set the pacing size if an external application, database, or the Data Integration Service node is a bottleneck. User lower values for faster performance.</p> <p>The minimum value and default value is 0. A value of 0 provides the best performance.</p>
Interpret as rows	<p>Optional. Select this option to express the pacing size as a number of rows. Clear this option to express the pacing size in kilobytes. By default, this option is not selected and the pacing size is in kilobytes.</p>
Compression	<p>Optional. Select this option to enable source data compression. By compressing data, you can decrease the amount of data that Informatica applications send over the network. By default, this option is not selected and compression is disabled.</p>
Offload processing	<p>Optional. Controls whether to offload some bulk data processing from the source machine to the Data Integration Service machine. Select one of the following options:</p> <ul style="list-style-type: none"> - AUTO. The Data Integration Service determines whether to use offload processing. - Yes. Use offload processing. - No. Do not use offload processing. <p>Default is AUTO.</p>
Worker threads	<p>Optional. Number of threads that the Data Integration Service uses to process bulk data when offload processing is enabled. For optimal performance, this value should not exceed the number of available processors on the Data Integration Service machine. Valid values are 1 through 64. Default is 0, which disables multithreading.</p>
Array size	<p>Optional. The number of records in the storage array for the worker threads. This option is applicable when you set the Worker Threads option to a value greater than 0. Valid values are 1 to 100000. Default is 25.</p>
Write mode	<p>Optional. Mode in which Data Integration Service sends data to the PowerExchange Listener. Select one of the following write modes:</p> <ul style="list-style-type: none"> - CONFIRMWRITEON. Sends data to the PowerExchange Listener and waits for a response before sending more data. Select this option when error recovery is a priority. However, this option might degrade performance. - CONFIRMWRITEOFF. Sends data to the PowerExchange Listener without waiting for a response. Use this option if you can reload the target table when an error occurs. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sends data to the PowerExchange Listener without waiting for a response. This option also enables error detection. This option combines the speed of CONFIRMWRITEOFF and the data integrity of CONFIRMWRITEON. <p>Default is CONFIRMWRITEON.</p>

JDBC Connection Properties

You can use a JDBC connection to access tables in a database. You can create and manage a JDBC connection in the Administrator tool, the Developer tool, or the Analyst tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes JDBC connection properties:

Property	Description
Database Type	The database type.
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	The description of the connection. The description cannot exceed 765 characters.
User Name	The database user name.
Password	The password for the database user name.
JDBC Driver Class Name	Name of the JDBC driver class. The following list provides the driver class name that you can enter for the applicable database type: <ul style="list-style-type: none">- DataDirect JDBC driver class name for Oracle: <code>com.informatica.jdbc.oracle.OracleDriver</code>- DataDirect JDBC driver class name for IBM DB2: <code>com.informatica.jdbc.db2.DB2Driver</code>- DataDirect JDBC driver class name for Microsoft SQL Server: <code>com.informatica.jdbc.sqlserver.SQLServerDriver</code>- DataDirect JDBC driver class name for Sybase ASE: <code>com.informatica.jdbc.sybase.SybaseDriver</code>- DataDirect JDBC driver class name for Informix: <code>com.informatica.jdbc.informix.InformixDriver</code>- DataDirect JDBC driver class name for MySQL: <code>com.informatica.jdbc.mysql.MySQLDriver</code> For more information about which driver class to use with specific databases, see the vendor documentation.
Connection String	Connection string to connect to the database. Use the following connection string: <code>jdbc:<subprotocol>:<subname></code>
Environment SQL	Optional. Enter SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the connection environment SQL each time it connects to the database.

Property	Description
Transaction SQL	Optional. Enter SQL commands to set the database environment when you connect to the database. The Data Integration Service executes the transaction environment SQL at the beginning of each transaction.
SQL Identifier Character	The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the Support Mixed-case Identifiers property.
Support Mixed-case Identifiers	When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. By default, this option is not selected.
Pass-through security enabled	Enables pass-through security for the connection. When you enable pass-through security for a connection, the domain uses the client user name and password to log into the corresponding database, instead of the credentials defined in the connection object.
Metadata Access Properties: Connection String	<p>The JDBC connection URL that is used to access metadata from the database.</p> <p>The following list provides the connection string that you can enter for the applicable database type:</p> <ul style="list-style-type: none"> - DataDirect JDBC driver for Oracle: jdbc:informatica:oracle://<hostname>:<port>;SID=<sid> - DataDirect JDBC driver for IBM DB2: jdbc:informatica:db2:// <hostname>:<port>;DatabaseName=<database name> - DataDirect JDBC driver for Microsoft SQL Server: jdbc:informatica:sqlserver:// <host>:<port>;DatabaseName=<database name> - DataDirect JDBC driver for Sybase ASE: jdbc:informatica:sybase:// <host>:<port>;DatabaseName=<database name> - DataDirect JDBC driver for Informix: jdbc:informatica:informix:// <host>:<port>;informixServer=<informix server name>;DatabaseName=<database name> - DataDirect JDBC driver for MySQL: jdbc:informatica:mysql:// <host>:<port>;DatabaseName=<database name> <p>For more information about the connection string to use for specific databases, see the vendor documentation for the URL syntax.</p>

Property	Description
AdvancedJDBCSecurityOptions	<p>Database parameters for metadata access to a secure database. Informatica treats the value of the AdvancedJDBCSecurityOptions field as sensitive data and stores the parameter string encrypted.</p> <p>To connect to a secure database, include the following parameters:</p> <ul style="list-style-type: none"> - EncryptionMethod. Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to SSL. - ValidateServerCertificate. Optional. Indicates whether Informatica validates the certificate that is sent by the database server. <p>If this parameter is set to True, Informatica validates the certificate that is sent by the database server. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate.</p> <p>If this parameter is set to false, Informatica does not validate the certificate that is sent by the database server. Informatica ignores any truststore information that you specify.</p> <ul style="list-style-type: none"> - HostNameInCertificate. Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate. - TrustStore. Required. Path and file name of the truststore file that contains the SSL certificate for the database. - TrustStorePassword. Required. Password for the truststore file for the secure database. <p>Not applicable for ODBC.</p> <p>Note: Informatica appends the secure JDBC parameters to the connection string. If you include the secure JDBC parameters directly to the connection string, do not enter any parameters in the AdvancedJDBCSecurityOptions field.</p>
Code Page	The code page used to read from a source database or to write to a target database or file.
Environment SQL	SQL commands to set the database environment when you connect to the database. The Data Integration Service runs the connection environment SQL each time it connects to the database.
Transaction SQL	SQL commands to set the database environment when you connect to the database. The Data Integration Service runs the transaction environment SQL at the beginning of each transaction.
Retry Period	This property is reserved for future use.
SQL Identifier Character	<p>The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the Support Mixed-case Identifiers property.</p> <p>Select the character based on the database in the connection.</p>
Support Mixed-case Identifiers	When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. By default, this option is not selected.

LinkedIn Connection Properties

Use a LinkedIn connection to extract data from the LinkedIn web site. A LinkedIn connection is a social media type connection. You can create and manage a LinkedIn connection in the Administrator tool or the Developer tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes LinkedIn connection properties:

Property	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	The description of the connection. The description cannot exceed 765 characters.
Location	The domain where you want to create the connection.
Type	The connection type. Select LinkedIn.
Do you have OAuth details?	Indicates whether you want to configure OAuth. Select one of the following values: - Yes. Indicates that you have the access token and secret. - No. Launches the OAuth Utility.
Consumer Key	The API key that you get when you create the application in LinkedIn. LinkedIn uses the key to identify the application.
Consumer Secret	The Secret key that you get when you create the application in LinkedIn. LinkedIn uses the secret to establish ownership of the consumer key.
Access Token	Access token that the OAuth Utility returns. The LinkedIn application uses this token instead of the user credentials to access the protected resources.
Access Secret	Access secret that the OAuth Utility returns. The secret establishes ownership of a token.
Scope	Optional. Permissions for the application. Enter the permissions that you used to configure OAuth.

MS SQL Server Connection Properties

Use a Microsoft SQL Server connection to access Microsoft SQL Server. A Microsoft SQL Server connection is a connection to a Microsoft SQL Server relational database. You can create and manage a Microsoft SQL Server connection in the Administrator tool or the Developer tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes MS SQL Server connection properties:

Property	Description
Database Type	The database type.
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	The description of the connection. The description cannot exceed 765 characters.
Use trusted connection	Enables the application service to use Windows authentication to access the database. The user name that starts the application service must be a valid Windows user with access to the database. By default, this option is cleared.
User Name	The database user name.
Password	The password for the database user name.
Pass-through security enabled	Enables pass-through security for the connection. When you enable pass-through security for a connection, the domain uses the client user name and password to log into the corresponding database, instead of the credentials defined in the connection object.
Metadata Access Properties: Connection String	Use the following connection URL: <code>jdbc:informatica:sqlserver://<host name>:<port>;DatabaseName=<database name></code>

Property	Description
AdvancedJDBCSecurityOptions	<p>Database parameters for metadata access to a secure database. Informatica treats the value of the AdvancedJDBCSecurityOptions field as sensitive data and stores the parameter string encrypted.</p> <p>To connect to a secure database, include the following parameters:</p> <ul style="list-style-type: none"> - EncryptionMethod. Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to SSL. - ValidateServerCertificate. Optional. Indicates whether Informatica validates the certificate that is sent by the database server. <p>If this parameter is set to True, Informatica validates the certificate that is sent by the database server. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate.</p> <p>If this parameter is set to false, Informatica does not validate the certificate that is sent by the database server. Informatica ignores any truststore information that you specify.</p> <ul style="list-style-type: none"> - HostNameInCertificate. Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate. - TrustStore. Required. Path and file name of the truststore file that contains the SSL certificate for the database. - TrustStorePassword. Required. Password for the truststore file for the secure database. <p>Not applicable for ODBC.</p> <p>Note: Informatica appends the secure JDBC parameters to the connection string. If you include the secure JDBC parameters directly to the connection string, do not enter any parameters in the AdvancedJDBCSecurityOptions field.</p>
Data Access Properties: Connection String	<p>Use the following connection string:</p> <pre><server name>@<database name></pre> <p>If the database does not use the default port, use the following connection strings:</p> <pre><server name>:<port>@<dbname> <servername>/<instancename>:<port>@<dbname></pre>
Code Page	The code page used to read from a source database or to write to a target database or file.
Domain Name	The name of the domain.
Packet Size	The packet size used to transmit data. Used to optimize the native drivers for Microsoft SQL Server.
Owner Name	The name of the owner of the schema.
Schema Name	The name of the schema in the database. You must specify the schema name for the Profiling Warehouse if the schema name is different from the database user name. You must specify the schema name for the data object cache database if the schema name is different from the database user name and you manage the cache with an external tool.
Environment SQL	SQL commands to set the database environment when you connect to the database. The Data Integration Service runs the connection environment SQL each time it connects to the database.

Property	Description
Transaction SQL	SQL commands to set the database environment when you connect to the database. The Data Integration Service runs the transaction environment SQL at the beginning of each transaction.
Retry Period	This property is reserved for future use.
SQL Identifier Character	The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the Support Mixed-case Identifiers property. Select the character based on the database in the connection.
Support Mixed-case Identifiers	When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. By default, this option is not selected.
ODBC Provider	ODBC. The type of database to which ODBC connects. For pushdown optimization, specify the database type to enable the Data Integration Service to generate native database SQL. The options are: <ul style="list-style-type: none"> - Other - Sybase - Microsoft_SQL_Server Default is Other.

ODBC Connection Properties

Use an ODBC connection to access ODBC data. An ODBC connection is a relational database connection. You can create and manage an ODBC connection in the Administrator tool, the Developer tool, or the Analyst tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes ODBC connection properties:

Property	Description
Database Type	The database type.
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	The description of the connection. The description cannot exceed 765 characters.

Property	Description
User Name	The database user name.
Password	The password for the database user name.
Pass-through security enabled	Enables pass-through security for the connection. When you enable pass-through security for a connection, the domain uses the client user name and password to log into the corresponding database, instead of the credentials defined in the connection object.
Data Access Properties: Connection String	The ODBC connection URL used to access metadata from the database. <data source name>
Code Page	The code page used to read from a source database or to write to a target database or file.
Environment SQL	SQL commands to set the database environment when you connect to the database. The Data Integration Service runs the connection environment SQL each time it connects to the database.
Transaction SQL	SQL commands to set the database environment when you connect to the database. The Data Integration Service runs the transaction environment SQL at the beginning of each transaction.
Retry Period	This property is reserved for future use.
SQL Identifier Character	The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the Support Mixed-case Identifiers property. Select the character based on the database in the connection.
Support Mixed-case Identifiers	When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. By default, this option is not selected.
ODBC Provider	The type of database to which ODBC connects. For pushdown optimization, specify the database type to enable the Data Integration Service to generate native database SQL. The options are: <ul style="list-style-type: none"> - Other - Sybase - Microsoft_SQL_Server Default is Other.

Oracle Connection Properties

Use an Oracle connection to connect to an Oracle database. The Oracle connection is a relational connection type. You can create and manage an Oracle connection in the Administrator tool, the Developer tool, or the Analyst tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes Oracle connection properties:

Property	Description
Database Type	The database type.
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	The description of the connection. The description cannot exceed 765 characters.
User Name	The database user name.
Password	The password for the database user name.
Pass-through security enabled	Enables pass-through security for the connection. When you enable pass-through security for a connection, the domain uses the client user name and password to log into the corresponding database, instead of the credentials defined in the connection object.
Metadata Access Properties: Connection String	Use the following connection URL: <code>jdbc:informatica:oracle:// <host_name>:<port>;SID=<database name></code>
AdvancedJDBCSecurityOptions	<p>Database parameters for metadata access to a secure database. Informatica treats the value of the AdvancedJDBCSecurityOptions field as sensitive data and stores the parameter string encrypted.</p> <p>To connect to a secure database, include the following parameters:</p> <ul style="list-style-type: none"> - EncryptionMethod. Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to SSL. - ValidateServerCertificate. Optional. Indicates whether Informatica validates the certificate that is sent by the database server. If this parameter is set to True, Informatica validates the certificate that is sent by the database server. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate. If this parameter is set to false, Informatica does not validate the certificate that is sent by the database server. Informatica ignores any truststore information that you specify. - HostNameInCertificate. Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate. - TrustStore. Required. Path and file name of the truststore file that contains the SSL certificate for the database. - TrustStorePassword. Required. Password for the truststore file for the secure database. <p>Note: Informatica appends the secure JDBC parameters to the connection string. If you include the secure JDBC parameters directly to the connection string, do not enter any parameters in the AdvancedJDBCSecurityOptions field.</p>

Property	Description
Data Access Properties: Connection String	Use the following connection string: <database name>.world
Code Page	The code page used to read from a source database or to write to a target database or file.
Environment SQL	SQL commands to set the database environment when you connect to the database. The Data Integration Service runs the connection environment SQL each time it connects to the database.
Transaction SQL	SQL commands to set the database environment when you connect to the database. The Data Integration Service runs the transaction environment SQL at the beginning of each transaction.
Retry Period	This property is reserved for future use.
Enable Parallel Mode	Enables parallel processing when loading data into a table in bulk mode. By default, this option is cleared.
SQL Identifier Character	The type of character used to identify special characters and reserved SQL keywords, such as WHERE. The Data Integration Service places the selected character around special characters and reserved SQL keywords. The Data Integration Service also uses this character for the Support Mixed-case Identifiers property. Select the character based on the database in the connection.
Support Mixed-case Identifiers	When enabled, the Data Integration Service places identifier characters around table, view, schema, synonym, and column names when generating and executing SQL against these objects in the connection. Use if the objects have mixed-case or lowercase names. By default, this option is not selected.

Salesforce Connection Properties

Use a Salesforce connection to connect to a Salesforce object. The Salesforce connection is an application connection type. You can create and manage a Salesforce connection in the Administrator tool or the Developer tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes Salesforce connection properties:

Property	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	The description of the connection. The description cannot exceed 765 characters.
Location	The Informatica domain where you want to create the connection.
Type	The connection type. Select Salesforce.
User Name	Salesforce user name.
User Password	Password for the Salesforce user name. To access Salesforce outside the trusted network of your organization, you must append a security token to your password to log in to the API or a desktop client. To receive or reset your security token, log in to Salesforce and click Setup > My Personal Information > Reset My Security Token . Password is case sensitive.
Service URL	URL of the Salesforce service you want to access. In a test or development environment, you might want to access the Salesforce Sandbox testing environment. For more information about the Salesforce Sandbox, see the Salesforce documentation.

SAP Connection Properties

Use an SAP connection to connect to an SAP data source. The SAP connection is an enterprise application connection type. You create this connection in the Developer tool. You can create and manage an SAP connection in the Administrator tool or the Developer tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes SAP connection properties:

Property	Description
User name	User name for the SAP source system.
Password	Password for the user name.

Property	Description
Trace	<p>Select this option to track the RFC calls that the SAP system makes. SAP stores the information about the RFC calls in a trace file.</p> <p>You can access the trace files from the following directories:</p> <ul style="list-style-type: none"> - <code>tomcat/bin</code> directory on the Informatica server machine - <code>clients/DeveloperClient</code> directory on the client machine
Connection type	Select Type A to connect to one SAP system. Select Type B when you want to use SAP load balancing.
Host name	Host name or IP address of the SAP server. Informatica uses this entry to connect to the SAP server.
R3 name	Name of the SAP system.
Group	Group name of the SAP application server.
System number	SAP system number.
Client number	SAP client number.
Language	Language that you want for the mapping. Must be compatible with the Developer tool code page. If you leave this option blank, Informatica uses the default language of the SAP system.
Code page	Code page compatible with the SAP server. Must also correspond to the language code.
Staging directory	Path in the SAP system where the staging file will be created.
Source directory	The Data Integration Service path containing the source file.
Use FTP	Enables FTP access to SAP.
FTP user	User name to connect to the FTP server.
FTP password	Password for the FTP user.
FTP host	<p>Host name or IP address of the FTP server.</p> <p>Optionally, you can specify a port number from 1 through 65535, inclusive. Default for FTP is 21. Use the following syntax to specify the host name:</p> <pre>hostname:port_number</pre> <p>Or</p> <pre>IP address:port_number</pre> <p>When you specify a port number, enable that port number for FTP on the host machine.</p> <p>If you enable SFTP, specify a host name or port number for an SFTP server. Default for SFTP is 22.</p>
Retry period	Number of seconds that the Data Integration Service attempts to reconnect to the FTP host if the connection fails. If the Data Integration Service cannot reconnect to the FTP host in the retry period, the session fails. Default value is 0 and indicates an infinite retry period.

Property	Description
Use SFTP	Enables SFTP access to SAP.
Public key file name	Public key file path and file name. Required if the SFTP server uses publickey authentication. Enabled for SFTP.
Private key file name	Private key file path and file name. Required if the SFTP server uses publickey authentication. Enabled for SFTP.
Private key file name password	Private key file password used to decrypt the private key file. Required if the SFTP server uses public key authentication and the private key is encrypted. Enabled for SFTP.

Sequential Connection Properties

Use a sequential connection to access sequential data sources. You create a sequential connection in the Developer tool. You can manage a sequential connection in the Administrator tool or the Developer tool.

A sequential data source is a data source that PowerExchange can access by using a data map defined with an access method of SEQ. The Data Integration Service connects to the data source through PowerExchange.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes Sequential connection properties:

Option	Description
Location	Node name for the location of the PowerExchange Listener that connects to the sequential data set. The node name is defined in the first parameter of the NODE statement in the PowerExchange dbmover.cfg configuration file.
User name	A user name that has the authority to access the sequential data set.

Option	Description
Password	<p>Password for the specified user name or a valid PowerExchange passphrase.</p> <p>A PowerExchange passphrase can be from 9 to 128 characters in length and can contain the following characters:</p> <ul style="list-style-type: none"> - Uppercase and lowercase letters - The numbers 0 to 9 - Spaces - The following special characters: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Note: The first character is an apostrophe.</p> <p>Passphrases cannot include single quotation marks ('), double quotation marks ("), or currency symbols.</p> <p>To use passphrases, ensure that the PowerExchange Listener runs with a security setting of SECURITY=(1,N) or higher in the DBMOVER member. For more information, see "SECURITY Statement" in the <i>PowerExchange Reference Manual</i>.</p> <p>The allowable characters in the IBM IRRPHREX exit do not affect the allowable characters in PowerExchange passphrases.</p> <p>Note: A valid RACF passphrase can be up to 100 characters in length. PowerExchange truncates passphrases longer than 100 characters when passing them to RACF for validation.</p>
Code page	Required. Name of the code page to use for reading from or writing to the sequential data set. Usually, this value is an ISO code page name, such as ISO-8859-6.
Pass-through security enabled	Enables pass-through security for the connection.
Encryption type	<p>Optional. The type of encryption that the Data Integration Service uses. Select one of the following options:</p> <ul style="list-style-type: none"> - None - RC2 - DES <p>Default is None.</p> <p>Notes:</p> <ul style="list-style-type: none"> - Informatica recommends that you use Secure Sockets Layer (SSL) authentication instead of configuring the Encryption Type and Level connection properties or the ENCRYPT and ENCRYPTLEVEL statements in the DBMOVER configuration file. SSL authentication provides stricter security and is used by several Informatica products. <p>For more information about implementing SSL authentication in a PowerExchange network, see the <i>PowerExchange Reference Manual</i>.</p> <ul style="list-style-type: none"> - The values that you select for the Encryption Type and Level connection attributes override the values in the ENCRYPT and ENCRYPTLEVEL statements, if defined, in the DBMOVER configuration file on the Integration Service machine. To enable encryption for a mapping, be sure to select the appropriate connection attributes.
[Encryption] Level	<p>If you selected RC2 or DES for Encryption Type, select one of the following options to indicate the encryption level that the Data Integration Service uses:</p> <ul style="list-style-type: none"> - 1. Use a 56-bit encryption key for DES and RC2. - 2. Use 168-bit triple encryption key for DES, and use a 64-bit encryption key for RC2. - 3. Use 168-bit triple encryption key for DES, and use a 128-bit encryption key for RC2. <p>This option is ignored if you do not select an encryption type.</p> <p>Default is 1.</p>

Option	Description
Pacing size	Optional. Amount of data that the source system can pass to the PowerExchange Listener. Set the pacing size if an external application, database, or the Data Integration Service node is a bottleneck. User lower values for faster performance. Minimum value and default value is 0. A value of 0 provides the best performance.
Interpret as rows	Optional Select this option to express the pacing size as a number of rows. Clear this option to express the pacing size in kilobytes. By default, this option is not selected and the pacing size is in kilobytes.
Compression	Optional. Select this option to enable source data compression. By compressing data, you can decrease the amount of data that Informatica applications send over the network. By default, this option is not selected and compression is disabled.
Offload processing	Optional. Controls whether to offload some bulk data processing from the source machine to the Data Integration Service machine. Select one of the following options: <ul style="list-style-type: none"> - AUTO. The Data Integration Service determines whether to use offload processing. - Yes. Use offload processing. - No. Do not use offload processing. Default is AUTO.
Worker threads	Optional. Number of threads that the Data Integration Service uses to process bulk data when offload processing is enabled. For optimal performance, this value should not exceed the number of available processors on the Data Integration Service machine. Valid values are 1 through 64. Default is 0, which disables multithreading.
Array size	Optional The number of records in the storage array for the worker threads. This option is applicable when you set the Worker Threads option to a value greater than 0. Valid values are 25 to 100000. Default is 25.
Write mode	Optional. Mode in which the Data Integration Service sends data to the PowerExchange Listener. Select one of the following write modes: <ul style="list-style-type: none"> - CONFIRMWRITEON. Sends data to the PowerExchange Listener and waits for a response before sending more data. Select this option when error recovery is a priority. However, this option might degrade performance. - CONFIRMWRITEOFF. Sends data to the PowerExchange Listener without waiting for a response. Use this option if you can reload the target table when an error occurs. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sends data to the PowerExchange Listener without waiting for a response. This option also enables error detection. This option combines the speed of CONFIRMWRITEOFF and the data integrity of CONFIRMWRITEON. Default is CONFIRMWRITEON.

Teradata Parallel Transporter Connection Properties

Use a Teradata connection to access Teradata tables. The Teradata connection is a database type connection. You can create and manage a Teradata connection in the Administrator tool or the Developer tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes Teradata connection properties:

Property	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	Description of the connection. The description cannot exceed 765 characters.
User Name	Teradata database user name with the appropriate write permissions to access the database.
Password	Password for the Teradata database user name.
Driver Name	Name of the Teradata JDBC driver.
Connection String	Use the following connection string: <code>jdbc:teradata://<hostname>/database=<database name>,tmode=ANSI,charset=UTF8</code>

The following table describes the properties for data access:

Property	Description
TDPID	Name or IP address of the Teradata database machine.
Database Name	Teradata database name. If you do not enter a database name, Teradata PT API uses the default login database name.
Data Code Page	Code page associated with the database. When you run a mapping that loads to a Teradata target, the code page of the Teradata PT connection must be the same as the code page of the Teradata target. Default is UTF-8.
Tenacity	Number of hours that Teradata PT API continues trying to log on when the maximum number of operations run on the Teradata database. Must be a positive, non-zero integer. Default is 4.
Max Sessions	Maximum number of sessions that Teradata PT API establishes with the Teradata database. Must be a positive, non-zero integer. Default is 4.

Property	Description
Min Sessions	Minimum number of Teradata PT API sessions required for the Teradata PT API job to continue. Must be a positive integer between 1 and the Max Sessions value. Default is 1.
Sleep	Number of minutes that Teradata PT API pauses before it retries to log on when the maximum number of operations run on the Teradata database. Must be a positive, non-zero integer. Default is 6.
Use Metadata JDBC URL for TDCH	Indicates that the Teradata Connector for Hadoop (TDCH) must use the JDBC URL that you specified in the connection string under the metadata access properties. Default is selected. Clear this option to enter a different JDBC URL that TDCH must use when it runs the mapping.
TDCH JDBC Url	Enter the JDBC URL that TDCH must use when it runs a Teradata mapping. Use the following format: <code>jdbc:teradata://<hostname>/database=<database name>, tmode=ANSI, charset=UTF8</code> This field is available only when you clear the Use Metadata JDBC URL for TDCH option.

Twitter Connection Properties

Use a Twitter connection to extract data from the Twitter web site. The Twitter connection is a connection to social media. You can create and manage a Twitter connection in the Administrator tool or the Developer tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes Twitter connection properties:

Property	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * () - + = { [] } \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	The description of the connection. The description cannot exceed 765 characters.
Location	The domain where you want to create the connection.

Property	Description
Type	The connection type. Select Twitter.
Do you have OAuth details?	Indicates whether you want to configure OAuth. Select one of the following values: <ul style="list-style-type: none"> - Yes. Indicates that you have the access token and secret. - No. Launches the OAuth Utility.
Consumer Key	The consumer key that you get when you create the application in Twitter. Twitter uses the key to identify the application.
Consumer Secret	The consumer secret that you get when you create the Twitter application. Twitter uses the secret to establish ownership of the consumer key.
Access Token	Access token that the OAuth Utility returns. Twitter uses this token instead of the user credentials to access the protected resources.
Access Secret	Access secret that the OAuth Utility returns. The secret establishes ownership of a token.

Twitter Streaming Connection Properties

Use a Twitter Streaming connection to access near-real time data from the Twitter web site. The Twitter Streaming connection is a connection to the social media company's streaming API. You can create and manage a Twitter Streaming connection in the Administrator tool or the Developer tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes the general properties for a Twitter Streaming connection:

Property	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * () - + = { [}] \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	The description of the connection. The description cannot exceed 765 characters.
Location	The domain where you want to create the connection.
Type	The connection type. Select Twitter Streaming.

The following table describes the properties for hose type and OAuth authentication:

Property	Description
Hose Type	Streaming API methods. You can specify one of the following methods: <ul style="list-style-type: none">- Filter. The Twitter <code>statuses/filter</code> method returns public statuses that match the search criteria.- Sample. The Twitter <code>statuses/sample</code> method returns a random sample of all public statuses.
Consumer Key	The consumer key that you get when you create the application in Twitter. Twitter uses the key to identify the application.
Consumer Secret	The consumer secret that you get when you create the Twitter application. Twitter uses the secret to establish ownership of the consumer key.
Do you have OAuth details?	Indicates whether you want to configure OAuth. Select one of the following values: <ul style="list-style-type: none">- Yes. Indicates that you have the access token and secret.- No. Launches the OAuth Utility.
Access Token	Access token that the OAuth Utility returns. Twitter uses the token instead of the user credentials to access the protected resources.
Access Secret	Access secret that the OAuth Utility returns. The secret establishes ownership of a token.

VSAM Connection Properties

Use a VSAM connection to access VSAM data tables. The VSAM connection is a flat file connection type. You create a VSAM connection in the Developer tool. You can manage a VSAM connection in the Administrator tool or the Developer tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes VSAM connection properties:

Option	Description
Location	Node name for the location of the PowerExchange Listener that connects to the VSAM data set. The node name is defined in the first parameter of the NODE statement in the PowerExchange <code>dbmover.cfg</code> configuration file.
User name	A user name that has the authority to connect to the VSAM data set.

Option	Description
Password	<p>A password for the specified user or a valid PowerExchange passphrase.</p> <p>A PowerExchange passphrase can be from 9 to 128 characters in length and can contain the following characters:</p> <ul style="list-style-type: none"> - Uppercase and lowercase letters - The numbers 0 to 9 - Spaces - The following special characters: ' - ; # \ , . / ! % & * () _ + { } : @ < > ? <p>Note: The first character is an apostrophe.</p> <p>Passphrases cannot include single quotation marks ('), double quotation marks ("), or currency symbols.</p> <p>To use passphrases, ensure that the PowerExchange Listener runs with a security setting of SECURITY=(1,N) or higher in the DBMOVER member. For more information, see "SECURITY Statement" in the <i>PowerExchange Reference Manual</i>.</p> <p>The allowable characters in the IBM IRRPHREX exit do not affect the allowable characters in PowerExchange passphrases.</p> <p>Note: A valid RACF passphrase can be up to 100 characters in length. PowerExchange truncates passphrases longer than 100 characters when passing them to RACF for validation.</p>
Code page	Required. Name of the code page to use for reading from or writing to the VSAM data set. Usually, this value is an ISO code page name, such as ISO-8859-6.
Pass-through security enabled	Enables pass-through security for the connection.
Encryption type	<p>Optional. The type of encryption that the Data Integration Service uses. Select one of the following options:</p> <ul style="list-style-type: none"> - None - RC2 - DES <p>Default is None.</p> <p>Notes:</p> <ul style="list-style-type: none"> - Informatica recommends that you use Secure Sockets Layer (SSL) authentication instead of configuring the Encryption Type and Level connection properties or the ENCRYPT and ENCRYPTLEVEL statements in the DBMOVER configuration file. SSL authentication provides stricter security and is used by several Informatica products. <p>For more information about implementing SSL authentication in a PowerExchange network, see the <i>PowerExchange Reference Manual</i>.</p> <ul style="list-style-type: none"> - The values that you select for the Encryption Type and Level connection attributes override the values in the ENCRYPT and ENCRYPTLEVEL statements, if defined, in the DBMOVER configuration file on the Integration Service machine. To enable encryption for a mapping, be sure to select the appropriate connection attributes.
[Encryption] Level	<p>If you selected RC2 or DES for Encryption Type, select one of the following options to indicate the encryption level that the Data Integration Service uses:</p> <ul style="list-style-type: none"> - 1. Use a 56-bit encryption key for DES and RC2. - 2. Use 168-bit triple encryption key for DES, and use a 64-bit encryption key for RC2. - 3. Use 168-bit triple encryption key for DES, and use a 128-bit encryption key for RC2. <p>This option is ignored if you do not select an encryption type.</p> <p>Default is 1.</p>

Option	Description
Pacing size	Optional. Amount of data that the source system can pass to the PowerExchange Listener. Set the pacing size if an external application, database, or the Data Integration Service node is a bottleneck. User lower values for faster performance. Minimum value and default value is 0. A value of 0 provides the best performance.
Interpret as rows	Optional. Select this option to express the pacing size as a number of rows. Clear this option to express the pacing size in kilobytes. By default, this option is not selected and the pacing size is in kilobytes.
Compression	Optional. Select this option to enable source data compression. By compressing data, you can decrease the amount of data that Informatica applications send over the network. By default, this option is not selected and compression is disabled.
Offload processing	Optional. Controls whether to offload some bulk data processing from the source machine to the Data Integration Service machine. Select one of the following options: <ul style="list-style-type: none"> - AUTO. The Data Integration Service determines whether to use offload processing. - Yes. Use offload processing. - No. Do not use offload processing. Default is AUTO.
Worker threads	Optional. Number of threads that the Data Integration Service uses to process bulk data when offload processing is enabled. For optimal performance, this value should not exceed the number of available processors on the Data Integration Service machine. Valid values are 1 through 64. Default is 0, which disables multithreading.
Array size	Optional. The number of records in the storage array for the worker threads. This option is applicable when you set the Worker Threads option to a value greater than 0. Valid values are 25 to 100000. Default is 25.
Write mode	Optional. Mode in which Data Integration Service sends data to the PowerExchange Listener. Select one of the following write modes: <ul style="list-style-type: none"> - CONFIRMWRITEON. Sends data to the PowerExchange Listener and waits for a response before sending more data. Select this option when error recovery is a priority. However, this option might degrade performance. - CONFIRMWRITEOFF. Sends data to the PowerExchange Listener without waiting for a response. Use this option if you can reload the target table when an error occurs. - ASYNCHRONOUSWITHFAULTTOLERANCE. Sends data to the PowerExchange Listener without waiting for a response. This option also enables error detection. This option combines the speed of CONFIRMWRITEOFF and the data integrity of CONFIRMWRITEON. Default is CONFIRMWRITEON.

Web Content-Kapow Katalyst Connection Properties

Use a Web Content-Kapow Katalyst connection to access robots in Kapow Katalyst. This is a social media type connection. You can create and manage a Web Content-Kapow Katalyst connection in the Administrator tool or the Developer tool.

Note: The order of the connection properties might vary depending on the tool where you view them.

The following table describes Web Content-Kapow Katalyst connection properties:

Property	Description
Name	Name of the connection. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters, contain spaces, or contain the following special characters: ~ ` ! \$ % ^ & * () - + = { [] \ : ; " ' < , > . ? /
ID	String that the Data Integration Service uses to identify the connection. The ID is not case sensitive. It must be 255 characters or less and must be unique in the domain. You cannot change this property after you create the connection. Default value is the connection name.
Description	The description of the connection. The description cannot exceed 765 characters.
Location	The Informatica domain where you want to create the connection.
Type	The connection type. Select Web Content-Kapow Katalyst.
Management Console URL	URL of the Management Console where the robot is uploaded. The URL must start with http or https. For example, http://localhost:50080.
RQL Service Port	The port number where the socket service listens for the RQL service. Enter a value from 1 through 65535. Default is 50000.
Username	User name required to access the Local Management Console.
Password	Password to access the Local Management Console.

Web Services Connection Properties

Use a web services connection to connect a Web Service Consumer transformation to a web service.

The following table describes the web services connection properties:

Property	Description
Username	User name to connect to the web service. Enter a user name if you enable HTTP authentication or WS-Security. If the Web Service Consumer transformation includes WS-Security ports, the transformation receives a dynamic user name through an input port. The Data Integration Service overrides the user name defined in the connection.
Password	Password for the user name. Enter a password if you enable HTTP authentication or WS-Security. If the Web Service Consumer transformation includes WS-Security ports, the transformation receives a dynamic password through an input port. The Data Integration Service overrides the password defined in the connection.

Property	Description
End Point URL	<p>URL for the web service that you want to access. The Data Integration Service overrides the URL defined in the WSDL file.</p> <p>If the Web Service Consumer transformation includes an endpoint URL port, the transformation dynamically receives the URL through an input port. The Data Integration Service overrides the URL defined in the connection.</p>
Timeout	Number of seconds that the Data Integration Service waits for a response from the web service provider before it closes the connection.
HTTP Authentication Type	<p>Type of user authentication over HTTP. Select one of the following values:</p> <ul style="list-style-type: none"> - None. No authentication. - Automatic. The Data Integration Service chooses the authentication type of the web service provider. - Basic. Requires you to provide a user name and password for the domain of the web service provider. The Data Integration Service sends the user name and the password to the web service provider for authentication. - Digest. Requires you to provide a user name and password for the domain of the web service provider. The Data Integration Service generates an encrypted message digest from the user name and password and sends it to the web service provider. The provider generates a temporary value for the user name and password and stores it in the Active Directory on the Domain Controller. It compares the value with the message digest. If they match, the web service provider authenticates you. - NTLM. Requires you to provide a domain name, server name, or default user name and password. The web service provider authenticates you based on the domain you are connected to. It gets the user name and password from the Windows Domain Controller and compares it with the user name and password that you provide. If they match, the web service provider authenticates you. NTLM authentication does not store encrypted passwords in the Active Directory on the Domain Controller.
WS Security Type	<p>Type of WS-Security that you want to use. Select one of the following values:</p> <ul style="list-style-type: none"> - None. The Data Integration Service does not add a web service security header to the generated SOAP request. - PasswordText. The Data Integration Service adds a web service security header to the generated SOAP request. The password is stored in the clear text format. - PasswordDigest. The Data Integration Service adds a web service security header to the generated SOAP request. The password is stored in a digest form which provides effective protection against replay attacks over the network. The Data Integration Service combines the password with a nonce and a time stamp. The Data Integration Service applies a SHA hash on the password, encodes it in base64 encoding, and uses the encoded password in the SOAP header.
Trust Certificates File	<p>File containing the bundle of trusted certificates that the Data Integration Service uses when authenticating the SSL certificate of the web service. Enter the file name and full directory path.</p> <p>Default is <Informatica installation directory>/services/shared/bin/ca-bundle.crt.</p>
Client Certificate File Name	Client certificate that a web service uses when authenticating a client. Specify the client certificate file if the web service needs to authenticate the Data Integration Service.
Client Certificate Password	Password for the client certificate. Specify the client certificate password if the web service needs to authenticate the Data Integration Service.

Property	Description
Client Certificate Type	<p>Format of the client certificate file. Select one of the following values:</p> <ul style="list-style-type: none"> - PEM. Files with the .pem extension. - DER. Files with the .cer or .der extension. <p>Specify the client certificate type if the web service needs to authenticate the Data Integration Service.</p>
Private Key File Name	Private key file for the client certificate. Specify the private key file if the web service needs to authenticate the Data Integration Service.
Private Key Password	Password for the private key of the client certificate. Specify the private key password if the web service needs to authenticate the Data Integration Service.
Private Key Type	Type of the private key. PEM is the supported type.

CHAPTER 8

Domain Object Export and Import

This chapter includes the following topics:

- [Domain Object Export and Import Overview, 138](#)
- [Export Process, 138](#)
- [View Domain Objects, 139](#)
- [Import Process, 146](#)

Domain Object Export and Import Overview

You can use the command line to migrate objects between two different domains of the same version.

You might migrate domain objects from a development environment to a test or production environment.

To export and import domain objects, use the following infacmd isp commands:

ExportDomainObjects

Exports native users, native groups, roles, and connections to an XML file.

ImportDomainObjects

Imports native users, native groups, roles, and connections into an Informatica domain.

You can use an infacmd control file to filter the objects during the export or import.

You can also use the infacmd xrf generateReadableViewXML command to generate a readable XML file from an export file. You can review the readable XML file to determine if you need to filter the objects that you import.

Export Process

You can use the command line to export domain objects from a domain.

Perform the following tasks to export domain objects:

1. Determine the domain objects that you want to export.
2. If you do not want to export all domain objects, create an export control file to filter the objects that are exported.
3. Run the infacmd isp exportDomainObjects command to export the domain objects.

The command exports the domain objects to an export file. You can use this file to import the objects into another domain.

Rules and Guidelines for Exporting Domain Objects

Review the following rules and guidelines before you export domain objects:

- When you export a user, by default, you do not export the user password. If you do not export the password, the administrator must reset the password for the user after the user is imported into the domain. However, when you run the `infacmd isp exportDomainObjects` command, you can choose to export an encrypted version of the password.
- When you export a user, you do not export the associated groups of the user. If applicable, assign the user to the group after you import the user and group.
- When you export a group, you export all sub-groups and users in the group.
- You cannot export the Administrator user, the Administrator role, the Everyone group, or LDAP users or groups. To replicate LDAP users and groups in an Informatica domain, import the LDAP users and groups directly from the LDAP directory service.
- To export native users and groups from domains of different versions, use the `infacmd isp exportUsersAndGroups` command.
- When you export a connection, by default, you do not export the connection password. If you do not export the password, the administrator must reset the password for the connection after the connection is imported into the domain. However, when you run the `infacmd isp exportDomainObjects` command, you can choose to export an encrypted version of the password.

View Domain Objects

You can view domain object names and properties in the export XML file.

Run `infacmd xrf generateReadableViewXML` command, to create a readable XML from the export file.

The following section provides a sample readable XML file:

```
<global:View xmlns:global="http://global" xmlns:connection="http://connection"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="
  http://connection connection.xsd http://global globalSchemaDomain.xsd http://global
  globalSchema.xsd">
  <NativeUser isAdmin="false" name="admin" securityDomain="Native" viewId="0">
    <UserInfo email="" fullName="admin" phone="" viewId="1"/>
  </NativeUser>
  <User isAdmin="false" name="User1" securityDomain="Native" viewId="15">
    <UserInfo email="" fullName="NewUSer" phone="" viewId="16"/>
  </User>
  <Group name="TestGroup1" securityDomain="Native" viewId="182">
    <UserRef name="User1" securityDomain="Native" viewId="183"/>
    <UserRef name="User6" securityDomain="Native" viewId="188"/>
  </Group>
  <Role customRole="false" name="Administrator" viewId="242">
    <Description viewId="243">Provides all privilege and permission access to an
    Informatica service.</Description>
    <ServicePrivilegeDefinition name="PwxListenerService" viewId="244">
      <Privilege category="" isEnabled="true" name="close" viewId="245"/>
      <Privilege category="" isEnabled="true" name="closeforce" viewId="246"/>
      <Privilege category="" isEnabled="false" name="Management Commands" viewId="249"/>
      <Privilege category="" isEnabled="false" name="Informational Commands"
      viewId="250"/>
    </ServicePrivilegeDefinition>
  </Role>
```

```

    <Connection connectionString="inqa85sql25@qa90"
connectionType="SQLServerNativeConnection"
    domainName="" environmentSQL="" name="conn4" ownerName=""
    schemaName="" transactionSQL="" userName="dummy" viewId="7512">
    <ConnectionPool maxIdleTime="120" minConnections="0" usePool="true" viewId="7514"/>
  </Connection>
</global:View>

```

Viewable Domain Object Names

You can view the following domain object names and properties in the readable XML file:

User

The following table lists the properties and the type:

Property	Type
name	string
securityDomain	string
admin	boolean
UserInfo	List<UserInfo>

UserInfo

The following table lists the properties and the type:

Property	Type
description	string
email	string
fullName	string
phone	string

Role

The following table lists the properties and the type:

Property	Type
name	string
description	string
customRole	boolean
servicePrivilege	List<ServicePrivilegeDef>

ServicePrivilegeDef

The following table lists the properties and the type:

Property	Type
name	string
privileges	List<Privilege>

Privilege

The following table lists the properties and the type:

Property	Type
name	string
enable	boolean
category	string

Group

The following table lists the properties and the type:

Property	Type
name	string
securityDomain	string
description	string
UserRefs	List<UserRef>

GroupRef

The following table lists the properties and the type:

Property	Type
name	string
securityDomain	string

UserRef

- name
- securityDomain

ConnectInfo

The following table lists the properties and the type:

Property	Type
id	string
name	string
connectionType	string
ConnectionPoolAttributes	List<ConnectionPoolAttributes>

ConnectionPoolAttributes

The following table lists the properties and the type:

Property	Type
maxIdleTime	int
minConnections	int
poolSize	int
usePool	boolean

Supported Connection Types

- DB2iNativeConnection
- DB2NativeConnection
- DB2zNativeConnection
- JDBCCConnection
- ODBCNativeConnection
- OracleNativeConnection
- PWXMetaConnection
- SAPConnection
- SDKConnection
- SQLServerNativeConnection
- SybaseNativeConnection
- TeradataNativeConnection
- URLLocation
- WebServiceConnection
- NRDBMetaConnection
- NRDBNativeConnection
- RelationalBaseSDKConnection

DB2iNativeConnection Properties

- connectionType
- connectionString
- username
- environmentSQL
- libraryList
- location
- databaseFileOverrides

DB2NativeConnection Properties

- connectionType
- connectionString
- username
- environmentSQL
- tableSpace
- transactionSQL

DB2zNativeConnection Properties

- connectionType
- connectionString
- username
- environmentSQL
- location

JDBCConnection Properties

- connectionType
- connectionString
- username
- dataStoreType

ODBCNativeConnection Properties

- connectionType
- connectionString
- username
- environmentSQL
- transactionSQL
- odbcProvider

OracleNativeConnection Properties

- connectionType
- connectionString
- username
- environmentSQL
- transactionSQL

PWXMetaConnection Properties

- connectionType
- databaseName
- userName
- dataStoreType
- dbType
- hostName
- location
- port

SAPConnection Properties

- connectionType
- userName
- description
- dataStoreType

SDKConnection Properties

- connectionType
- sdkConnectionType
- dataSourceType

SQLServerNativeConnection Properties

- connectionType
- connectionString
- username
- environmentSQL
- transactionSQL
- domainName
- ownerName
- schemaName

TeradataNativeConnection Properties

- connectionType
- username
- environmentSQL
- transactionSQL
- dataSourceName
- databaseName

TeradataNativeConnection Properties

- connectionType
- username
- environmentSQL
- transactionSQL

- connectionString

URLLocation Properties

- connectionType
- locatorURL

WebServiceConnection Properties

- connectionType
- url
- userName
- wsseType
- httpAuthenticationType

NRDBNativeConnection Properties

- connectionType
- userName
- location

NRDBMetaConnection Properties

- connectionType
- username
- location
- dataStoreType
- hostName
- port
- databaseType
- databaseName
- extensions

RelationalBaseSDKConnection Properties

- connectionType
- databaseName
- connectionString
- domainName
- environmentSQL
- hostName
- owner
- ispSvcName
- metadataDataStorageType
- metadataConnectionString
- metadataConnectionUserName

Import Process

You can use the command line to import domain objects from an export file into a domain.

Perform the following tasks to import domain objects:

1. Run the `infacmd xrf generateReadableViewXML` command to generate a readable XML file from an export file. Review the domain objects in the readable XML file and determine the objects that you want to import.
2. If you do not want to import all domain objects in the export file, create an import control file to filter the objects that are imported.
3. Run the `infacmd isp importDomainObjects` command to import the domain objects into the specified domain.
4. After you import the objects, you may still have to create other domain objects such as application services and folders.

Rules and Guidelines for Importing Domain Objects

Review the following rules and guidelines before you import domain objects.

- When you import a group, you import all sub-groups and users in the group.
- To import native users and groups from domains of different versions, use the `infacmd isp importUsersAndGroups` command.
- After you import a user or group, you cannot rename the user or group.
- You import roles independently of users and groups. Assign roles to users and groups after you import the roles, users, and groups.
- You cannot import the Administrator group, Administrator user, the Administrator role, the Everyone group, or LDAP users or groups

Conflict Resolution

A conflict occurs when you try to import an object with a name that exists for an object in the target domain. Configure the conflict resolution to determine how to handle conflicts during the import.

You can define a conflict resolution strategy through the command line or control file when you import the objects. The control file takes precedence if you define conflict resolution in the command line and control file. The import fails if there is a conflict and you did not define a conflict resolution strategy.

You can configure one of the following conflict resolution strategies:

Reuse

Reuses the object in the target domain.

Rename

Renames the source object. You can provide a name in the control file, or else the name is generated. A generated name has a number appended to the end of the name.

Replace

Replaces the target object with the source object.

Merge

Merges the source and target objects into one group. For example, if you merge groups with the same name, users and sub-groups from both groups are merged into the group in the target domain.

You cannot define the merge conflict resolution strategy through the command line. Use a control file to define the merge conflict resolution strategy. You must include the group object type section with merge as the conflict resolution policy with reuse, replace, or rename for all conflicting users in the control file.

For example, specify the merge conflict resolution strategy for the following groups:

- Group A with users a1, a2, b1, b2 in the source domain.
- Group A with users a1, a2, a3 b1, b2 in the target domain

You get the following results in the group after merge in the target domain:

- a1, a2, b1, b2 if you choose reuse or replace
- a1, a2, a3, b1, b2 if you choose rename.

CHAPTER 9

License Management

This chapter includes the following topics:

- [License Management Overview, 148](#)
- [Types of License Keys, 150](#)
- [Creating a License Object, 151](#)
- [Assigning a License to a Service, 152](#)
- [Unassigning a License from a Service, 152](#)
- [Updating a License, 153](#)
- [Removing a License, 153](#)
- [License Properties, 154](#)

License Management Overview

The Service Manager on the master gateway node manages Informatica licenses.

A license enables you to perform the following tasks:

- Run application services, such as the Analyst Service, Data Integration Service, and PowerCenter Repository Service.
- Use add-on options, such as partitioning for PowerCenter, grid, and high availability.
- Access particular types of connections, such as Oracle, Teradata, Microsoft SQL Server, and IBM MQ Series.
- Use Metadata Exchange options, such as Metadata Exchange for Cognos and Metadata Exchange for Rational Rose.

When you install Informatica, the installation program creates a license object in the domain based on the license key that you used during installation.

You assign a license object to each application service to enable the service. For example, you must assign a license to the PowerCenter Integration Service before you can use the PowerCenter Integration Service to run a workflow.

You can create additional license objects in the domain. Based on your project requirements, you may need multiple license objects. For example, you may have two license objects, where each license object allows you to run services on a different operating system. You might also use multiple license objects to manage multiple projects in the same domain. One project may require access to particular database types, while the other project does not.

License Validation

The Service Manager validates application service processes when they start. The Service Manager validates the following information for each service process:

- Product version. Verifies that you are running the appropriate version of the Informatica services.
- Platform. Verifies that the Informatica services are running on a licensed operating system.
- Expiration date. Verifies that the license is not expired. If the license expires, no application service assigned to the license can start. You must assign a valid license to the Informatica services to start them.
- PowerCenter options. Determines the options that the Informatica services have permission to use. For example, the Service Manager verifies if the PowerCenter Integration Service can use the Session on Grid option.
- Connectivity. Verifies connections that the Informatica services have permission to use. For example, the Service Manager verifies that PowerCenter can connect to a IBM DB2 database.
- Metadata Exchange options. Determines the Metadata Exchange options that are available for use. For example, the Service Manager verifies that you have access to the Metadata Exchange for Business Objects Designer.

Licensing Log Events

The Service Manager generates log events and writes them to the Log Manager. It generates log events for the following actions:

- You create or delete a license.
- You apply an incremental license key to a license.
- You assign an application service to a license.
- You unassign a license from an application service.
- The license expires.
- The Service Manager encounters an error, such as a validation error.

The log events include the user name and the time associated with the event.

You must have permission on the domain to view the logs for Licensing events.

The Licensing events appear in the domain logs.

License Management Tasks

You can perform the following tasks to manage the licenses:

- Create the license in the Administrator tool. You use a license key to create a license in the Administrator tool.
- Assign a license to each application service. Assign a license to each application service to enable the service.
- Unassign a license from an application service. Unassign a license from an application service if you want to discontinue the service or migrate the service from a development environment to a production environment. After you unassign a license from a service, you cannot enable the service until you assign another valid license to it.
- Update the license. Update the license to add PowerCenter options to the existing license.
- Remove the license. Remove a license if it is obsolete.
- Configure user permissions on a license.

- View license details. You may need to review the licenses to determine details, such as expiration date and the maximum number of licensed CPUs. You may want to review these details to ensure you are in compliance with the license. Use the Administrator tool to determine the details for each license.
- Monitor license usage and licensed options. You can monitor the usage of logical CPUs and PowerCenter Repository Services. You can monitor the number of software options purchased for a license and the number of times a license exceeds usage limits in the License Management Report.

You can perform all of these tasks in the Administrator tool or by using *infacmd isp* commands.

Types of License Keys

Informatica provides license keys in license files. The license key is encrypted. When you create the license from the license key file, the Service Manager decrypts the license key and enables the purchased options.

You create a license from a license key file. You apply license keys to the license to enable additional options. Informatica uses the following types of license keys:

- Original keys. Informatica generates an original key based on your contract. Informatica may provide multiple original keys depending on your contract.
- Incremental keys. Informatica generates incremental keys based on updates to an existing license, such as an extended license period or an additional option.

Note: Informatica licenses typically change with each version. Use a license key file valid for the current version to ensure that your installation includes all functionality.

Original Keys

Original keys identify the contract, product, and licensed features. Licensed features include the Informatica edition, deployment type, number of authorized CPUs, and authorized Informatica options and connectivity. You use the original keys to install Informatica and create licenses for services. You must have a license key to install Informatica. The installation program creates a license object for the domain in the Administrator tool. You can use other original keys to create more licenses in the same domain. You use a different original license key for each license object.

Incremental Keys

You use incremental license keys to update an existing license. You add an incremental key to an existing license to add or remove options, such as PowerCenter options, connectivity, and Metadata Exchange options. For example, if an existing license does not allow high availability, you can add an incremental key with the high availability option to the existing license.

The Service Manager updates the license expiration date if the expiration date of an incremental key is later than the expiration date of an original key. The Service Manager uses the latest expiration date. A license object can have different expiration dates for options in the license. For example, the IBM DB2 relational connectivity option may expire on 12/01/2006, and the session on grid option may expire on 04/01/06.

The Service Manager validates the incremental key against the original key used to create the license. An error appears if the keys are not compatible.

Creating a License Object

You can create a license object in a domain and assign the license to application services. You can create the license in the Administrator tool using a license key file. The license key file contains an encrypted original key. You use the original key to create the license.

You can also use the *infacmd isp AddLicense* command to add a license to the domain.

Use the following guidelines to create a license:

- Use a valid license key file. The license key file must contain an original license key. The license key file must not be expired.
- You cannot use the same license key file for multiple licenses. Each license must have a unique original key.
- Enter a unique name for each license. You create a name for the license when you create the license. The name must be unique among all objects in the domain.
- Put the license key file in a location that is accessible by the Administrator tool computer. When you create the license object, you must specify the location of the license key file.

After you create the license, you can change the description. To change the description of a license, select the license in Navigator of the Administrator tool, and then click Edit.

1. In the Administrator tool, click **Actions > New > License**.

The **Create License** window appears.

2. Enter the following options:

Option	Description
Name	Name of the license. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! () []
Description	Description of the license. The description cannot exceed 765 characters.
Path	Path of the domain in which you create the license. Read-only field. Optionally, click Browse and select a domain in the Select Folder window. Optionally, click Create Folder to create a folder for the domain.
License File	File containing the original key. Click Browse to locate the file.

If you try to create a license using an incremental key, a message appears that states you cannot apply an incremental key before you add an original key.

You must use an original key to create a license.

3. Click **Create**.

Assigning a License to a Service

Assign a license to an application service before you can enable the service. When you assign a license to a service, the Service Manager updates the license metadata. You can also use the *infacmd isp AssignLicense* command to assign a license to a service.

1. Select the license in the **Navigator** of the Administrator tool.
2. Click the **Assigned Services** tab.
3. In the **License** tab, click **Actions > Edit Assigned Services**.

The **Assign or Unassign this license to the services** window appears.

4. Select the services under **Unassigned Services**, and click **Add**.

Use Ctrl-click to select multiple services. Use Shift-click to select a range of services. Optionally, click **Add all** to assign all services.

5. Click **OK**.

Rules and Guidelines for Assigning a License to a Service

Use the following rules and guidelines when you assign licenses:

- You can assign licenses to disabled services.
- If you want to assign a license to a service that has a license assigned to it, you must first unassign the existing license from the service.
- To start a service with backup nodes, you must assign it to a license with high availability.
- To restart a service automatically, you must assign the service to a license with high availability.

Unassigning a License from a Service

You might need to unassign a license from a service if the service becomes obsolete or if you want to discontinue a service. You might want to discontinue a service if you are using more CPUs than you are licensed to use.

You can use the Administrator tool or the *infacmd isp UnassignLicense* command to unassign a license from a service.

You must disable a service before you can unassign a license from it. After you unassign the license from the service, you cannot enable the service. You must assign a valid license to the service to reen able it.

You must disable the service before you can unassign the license. If you try to unassign a license from an enabled service, a message appears that states you cannot remove the service because it is running.

1. Select the license in the **Navigator** of the Administrator tool.
2. Click the **Assigned Services** tab.
3. In the **License** tab, click **Actions > Edit Assigned Services**.

The **Assign or Unassign this license to the services** window appears.

4. Select the service under **Assigned Services**, and then click **Remove**. Optionally, click **Remove all** to unassign all assigned services.

5. Click **OK**.

Updating a License

You can update the current license in the Informatica domain with an incremental license key.

When you add an incremental key to a license, the Service Manager adds or removes licensed options and updates the license expiration date.

You can also use the *infacmd isp UpdateLicense* command to add an incremental key to a license.

After you update the license you must restart Informatica Services for the changes to take effect.

Use the following guidelines to update a license:

- Verify that the license key file is accessible by the Administrator tool computer. When you update the license object, you must specify the location of the license key file.
- The incremental key must be compatible with the original key. An error appears if the keys are not compatible.

The Service Manager validates the license key against the original key based on the following information:

- Serial number
- Deployment type
- Distributor
- Informatica edition
- Informatica version

1. Select a **license** in the Navigator.
2. Click the **Properties** tab.
3. In the **License** tab, click **ActionsActions > Add Incremental Key**.

The **Update License** window appears.

4. Click **Browse** to select the license key file. Optionally, you can enter the path to the license key.
5. Click **OK**.
6. In the **License Details** section of the **Properties** tab, click **Edit** to edit the description of the license.
7. Click **OK**.

Removing a License

You can remove a license from a domain using the Administrator tool or the *infacmd isp RemoveLicense* command.

Before you remove a license, disable all services assigned to the license. If you do not disable the services, all running service processes abort when you remove the license. When you remove a license, the Service Manager unassigns the license from each assigned service and removes the license from the domain. To re-enable a service, assign another license to it.

If you remove a license, you can still view License Usage logs in the Log Viewer for this license, but you cannot run the License Report on this license.

To remove a license from the domain:

1. Select the license in the **Navigator** of the Administrator tool.

2. Click **Actions > Delete**.

License Properties

You can view license details using the Administrator tool or the `infacmd isp ShowLicense` command.

The license details are based on all license keys applied to the license. The Service Manager updates the existing license details when you add a new incremental key to the license.

You might review license details to determine options that are available for use. You may also review the license details and license usage logs when monitoring licenses.

For example, you can determine the number of CPUs your company is licensed to use for each operating system.

To view license details, select the license in the **Navigator**.

The Administrator tool displays the license properties in the following sections:

- **License Details.** View license details on the **Properties** tab. Shows license attributes, such as the license object name, description, and expiration date.
- **Supported Platforms.** View supported platforms on the **Properties** tab. Shows the operating systems and how many CPUs are supported for each operating system.
- **Repositories.** View the licensed repositories on the **Properties** tab. Shows the maximum number of licensed repositories.
- **Assigned Services.** View application services that are assigned to the license on the **Assigned Services** tab.
- **PowerCenter Options.** View the PowerCenter options on the **Options** tab. Shows all licensed PowerCenter options, such as session on grid, high availability, and pushdown optimization.
- **Connections.** View the licensed connections on the **Options** tab. Shows all licensed connections. The license enables you to use connections, such as DB2 and Oracle database connections.
- **Metadata Exchange Options.** View the Metadata Exchange options on the **Options** tab. Shows a list of all licensed Metadata Exchange options, such as Metadata Exchange for Business Objects Designer.

You can also run the License Management Report to monitor licenses.

License Details

You can use the license details to view high-level information about the license. Use this license information when you audit the licensing usage.

The general properties for the license appear in the **License Details** section of the **Properties** tab.

The following table describes the general properties for a license:

Property	Description
Name	Name of the license.
Description	Description of the license.

Property	Description
Location	Path to the license in the Navigator.
Edition	PowerCenter Advanced edition.
License Version	Version of license.
Distributed By	Distributor of the product.
Issued On	Date when the license was issued to the customer.
Expires On	Date when the license expires.
Validity Period	Period for which the license is valid.
Serial Number	Serial number of the license. The serial number identifies the customer or project. If you have multiple PowerCenter installations, there is a separate serial number for each project. The original and incremental keys for a license have the same serial number.
Deployment Level	Level of deployment. Values are "Development" and "Production."

You can also use the license event logs to view audit summary reports. You must have permission on the domain to view the logs for license events.

Supported Platforms

You assign a license to each service. The service can run on any operating system supported by the license. One product license can support multiple operating system platforms.

The supported platforms for the license appear in the Supported Platforms section of the **Properties** tab.

The following table describes the supported platform properties for a license:

Property	Description
Description	Name of the supported operating system.
Logical CPUs	Number of CPUs you can run on the operating system.
Issued On	Date on which the license was issued.
Expires	Date on which the license expires.

Repositories

The maximum number of active repositories for the license appear in the Repositories section of the Properties tab.

The following table describes the repository properties for a license:

Property	Description
Description	Name of the repository.
Instances	Number of repository instances running on the operating system.
Issued On	Date on which the license was issued for this option.
Expires	Date on which the license expires for this option.

Service Options

The license enables you to use Informatica Service options such as data cleansing, data federation, and pushdown optimization.

The options for the license appear in the Service Options section of the **Options** tab.

Connections

The license enables you to use connections such as DB2 and Oracle database connections. The license also enables you to use connections for PowerExchange adapters such as PowerExchange for Facebook.

The connections for the license appear in the Connections section of the **Options** tab.

Metadata Exchange Options

The license enables you to use Metadata Exchange options such as Metadata Exchange for Business Objects Designer and Metadata Exchange for Microstrategy.

The Metadata Exchange options for the license appear in the Metadata Exchange Options section of the **Options** tab.

CHAPTER 10

Log Management

This chapter includes the following topics:

- [Log Management Overview, 157](#)
- [Log Manager Architecture, 158](#)
- [Log Location, 159](#)
- [Log Management Configuration, 160](#)
- [Using the Logs Tab, 161](#)
- [Log Events, 166](#)
- [Log Aggregator, 171](#)

Log Management Overview

The Service Manager provides accumulated log events for the domain, application services, users, and PowerCenter sessions and workflows. To perform the logging function, the Service Manager runs a Log Manager and a Log Agent.

The Log Manager runs on the master gateway node. It collects and processes log events for Service Manager domain operations, application services, and user activity. The log events contain operational and error messages for a domain. The Service Manager and the application services send log events to the Log Manager. When the Log Manager receives log events, it generates log event files. You can view service log events in the Administrator tool based on criteria you provide.

The Log Agent runs on all nodes in the domain. The Log Agent retrieves the workflow and session log events written by the PowerCenter Integration Service to display in the Workflow Monitor. Workflow log events include information about tasks performed by the PowerCenter Integration Service, workflow processing, and workflow errors. Session log events include information about the tasks performed by the PowerCenter Integration Service, session errors, and load summary and transformation statistics for the session. You can view log events for the last workflow run with the Log Events window in the Workflow Monitor.

The Log Agent runs on the nodes to collect and process log events for profile jobs, scorecard jobs, preview jobs, mapping jobs, and SQL Data Services for each Data Integration Service. You can view log events for profile jobs, scorecard jobs, preview jobs, mapping jobs, and SQL Data Services on the Monitoring tab.

Log event files are binary files that the Administrator tool Logs Viewer uses to display log events. When you view log events in the Administrator tool, the Log Manager uses the log event files to display the log events for the domain, application services, and user activity.

You can use the Administrator tool to perform the following tasks with the Log Manager:

- Configure the log location. Configure the node that runs the Log Manager, the directory path for log event files, purge options, and time zone for log events.
- Configure log management. Configure the Log Manager to purge logs or purge logs manually. Save log events to XML, text, or binary files. Configure the time zone for the time stamp in the log event files.
- View log events. View domain function, application service, and user activity log events on the Logs tab. Filter log events by domain, application service type, and user.

Log Manager Architecture

The Service Manager on the master gateway node controls the Log Manager. The Log Manager starts when you start the Informatica services. After the Log Manager starts, it listens for log events from the Service Manager and application services. When the Log Manager receives log events, it generates log event files.

The Log Manager creates the following types of log files:

- Log events files. Stores log events in binary format. The Log Manager creates log event files to display log events in the Logs tab. When you view events in the Administrator tool, the Log Manager retrieves the log events from the event nodes.

The Log Manager stores the files by date and by node. You configure the directory path for the Log Manager in the Administrator tool when you configure gateway nodes for the domain. By default, the directory path is the `server\logs` directory.

- Guaranteed Message Delivery files. Stores domain, application service, and user activity log events. The Service Manager writes the log events to temporary Guaranteed Message Delivery files and sends the log events to the Log Manager.

If the Log Manager becomes unavailable, the Guaranteed Message Delivery files stay in the `server\tomcat\logs` directory on the node where the service runs. When the Log Manager becomes available, the Service Manager for the node reads the log events in the temporary files, sends the log events to the Log Manager, and deletes the temporary files.

PowerCenter Session and Workflow Log Events

PowerCenter session and workflow logs are stored in a separate location from the domain, application service, and user activity logs. The PowerCenter Integration Service writes session and workflow log events to binary files on the node where the PowerCenter Integration Service runs.

The Log Manager performs the following tasks to process PowerCenter session and workflow log events:

1. During a session or workflow, the PowerCenter Integration Service writes binary log files on the node. It sends information about the logs to the Log Manager.
2. The Log Manager stores information about workflow and session logs in the domain database. The domain database stores information such as the path to the log file location, the node that contains the log, and the PowerCenter Integration Service that created the log.
3. When you view a session or workflow in the Log Events window of the Workflow Monitor, the Log Manager retrieves the information from the domain database. The Log Manager uses the information to determine the location of the logs.
4. The Log Manager dispatches a Log Agent to retrieve the log events on each node to display in the Log Events window.

Log Manager Recovery

When a service generates log events, it sends them to the Log Manager on the master gateway node. When you have the high availability option and the master gateway node becomes unavailable, the application services send log events to the Log Manager on a new master gateway node.

The Service Manager, the application services, and the Log Manager perform the following tasks:

1. An application service process writes log events to a Guaranteed Message Delivery file.
2. The application service process sends the log events to the Service Manager on the gateway node for the domain.
3. The Log Manager processes the log events and writes log event files. The application service process deletes the temporary file.
4. If the Log Manager is unavailable, the Guaranteed Message Delivery files stay on the node running the service process. The Service Manager for the node sends the log events in the Guaranteed Message Delivery files when the Log Manager becomes available, and the Log Manager writes log event files.

Troubleshooting the Log Manager

Domain and application services write log events to Service Manager log files when the Log Manager cannot process log events. The Service Manager log files are located in the `server\tomcat\logs` directory. The Service Manager log files include `catalina.out`, `localhost_<date>.txt`, and `node.log`. Services write log events to different log files depending on the type of error.

Use the Service Manager log files to troubleshoot issues when the Log Manager cannot process log events. You will also need to use these files to troubleshoot issues when you contact Informatica Global Customer Support.

Note: You can troubleshoot an Informatica installation by reviewing the log files generated during installation. You can use the installation summary log file to find out which components failed during installation.

Log Location

The Service Manager on the master gateway node writes domain, application service, and user activity log event files to the log file directory. When you configure a node to serve as a gateway, you must configure the directory where the Service Manager on this node writes the log event files. Each gateway node must have access to the directory path.

You configure the log location in the Properties view for the domain. Configure a directory location that is accessible to the gateway node during installation or when you define the domain. Store the logs on a shared disk when you have more than one gateway node. If the Log Manager is unable to write to the directory path, it writes log events to `node.log` on the master gateway node.

By default, the directory path is the `server\logs` directory. When you configure the log location, the Administrator tool validates the directory as you update the configuration. If the directory is invalid, the update fails. The Log Manager verifies that the log directory has read/write permissions on startup. Log files might contain inconsistencies if the log directory is not shared in a highly available environment.

If you have multiple Informatica domains, you must configure a different directory path for the Log Manager in each domain. Multiple domains cannot use the same shared directory path.

Note: When you change the directory path, you must restart Informatica Services on the node you changed.

Log Management Configuration

The Service Manager and the application services continually send log events to the Log Manager. As a result, the directory location for the logs can grow to contain a large number of log events.

You can purge logs events periodically to manage the amount of log events stored by the Log Manager. You can export logs before you purge them to keep a backup of the log events.

Purging Log Events

You can automatically or manually purge log events. The Service Manager purges log events from the log directory according to the purge properties you configure in the Log Management dialog box. You can manually purge log events to override the automatic purge properties.

Purging Log Events Automatically

The Service Manager purges log events from the log directory according to the purge properties. The default value for preserving logs is 30 days and the default maximum size for log event files is 200 MB.

When the number of days or the size of the log directory exceeds the limit, the Log Manager deletes the log event files, starting with the oldest log events. The Log Manager periodically verifies the purge options and purges log events. The Log Manager does not purge the current day log event files and folder.

Note: The Log Manager does not purge PowerCenter session and workflow log files.

Purging Log Events Manually

You can purge log events for the domain, application services, or user activity. When you purge log events, the Log Manager removes the log event files from the log directory. The Log Manager does not remove log event files currently being written to the logs.

Optionally, you can use the *infacmd* PurgeLog command to purge log events.

The following table lists the purge log options:

Option	Description
Log Type	Type of log events to purge. You can purge domain, service, user activity or all log events.
Service Type	When you purge application service log events, you can purge log events for a particular application service type or all application service types.
Purge Entries	Date range of log events you want to purge. You can select the following options: <ul style="list-style-type: none">- All Entries. Purges all log events.- Before Date. Purges log events that occurred before this date. Use the yyyy-mm-dd format when you enter a date. Optionally, you can use the calendar to choose the date. To use the calendar, click the date field.

Time Zone

When the Log Manager creates log event files, it generates a time stamp based on the time zone for each log event. When the Log Manager creates log folders, it labels folders according to a time stamp. When you export or purge log event files, the Log Manager uses this property to calculate which log event files to purge or export. Set the time zone to the location of the machine that stores the log event files.

Verify that you do not lose log event files when you configure the time zone for the Log Manager. If the application service that sends log events to the Log Manager is in a different time zone than the master gateway node, you may lose log event files you did not intend to delete. Configure the same time zone for each gateway node.

Note: When you change the time zone, you must restart Informatica Services on the node that you changed.

Configuring Log Management Properties

Configure the Log Management properties in the Log Management dialog box.

1. In the Administrator tool, click the Logs tab.
2. On the Log Actions menu, click Log Management.
3. Enter the number of days for the Log Manager to preserve log events.
4. Enter the maximum disk size for the directory that contains the log event files.
5. Enter the time zone in the following format:
`GMT (+|-)<hours>:<minutes>`
For example: GMT+08:00
6. Click OK.

Using the Logs Tab

You can view domain, application service, and user activity log events in the Logs tab of the Administrator tool. When you view log events in the Logs tab, the Log Manager displays the generated log event files in the log directory. When an error message appears in the Administrator tool, the error provides a link to the Logs tab.

You can use the Logs tab to perform the following tasks:

- View log events and the Administrator tool operational errors. View log events for the domain, an application service, or user activity.
- Filter log event results. After you display the log events, you can display log events that match filter criteria.
- Configure columns. Configure the columns you want the Logs tab to display.
- Save log events. You can save log events in XML, text, and binary format.
- Purge log events. You can manually purge log events.
- Copy log event rows. You can copy log event rows.

Viewing Log Events

To view log events in the Logs tab of the Administrator tool, select the Domain, Service, or User Activity view. Next, configure the filter options. You can filter log events based on attributes such as log type, domain function category, application service type, application service name, user, message code, activity code, timestamp, and severity level. The available options depend on whether you choose to view domain, application service, or user activity log events.

To view more information about a log event, click the log event in the search results.

On AIX and Linux, if the Log Manager receives an internal error message from the PowerCenter Integration Service, it writes a stack trace to the log event window.

You can view logs to get more information about errors that you receive while working in the Administrator tool.

1. In the Administrator Tool, click the Logs tab.
2. In the contents panel, select Domain, Service, or User Activity view.
3. Configure the filter criteria to view a specific type of log event.

The following table lists the query options:

Log Type	Option	Description
Domain	Category	Category of domain service you want to view.
Service	Service Type	Application service you want to view.
Service	Service Name	Name of the application service for which you want to view log events. You can choose a single application service name or all application services.
Domain, Service	Severity	The Log Manager returns log events with this severity level.
User Activity	User	User name for the Administrator tool user.
User Activity	Security Domain	Security domain to which the user belongs.
Domain, Service, User Activity	Timestamp	Date range for the log events that you want to view. You can choose the following options: <ul style="list-style-type: none"> - Blank. View all log events. - Within Last Day - Within Last Month - Custom. Specify the start and end date. Default is Within Last Day.
Domain, Service	Thread	Filter criteria for text that appears in the thread data. You can use wildcards (*) in this text field.
Domain, Service	Message Code	Filter criteria for text that appears in the message code. You can also use wildcards (*) in this text field.
Domain, Service	Message	Filter criteria for text that appears in the message. You can also use wildcards (*) in this text field.
Domain, Service	Node	Name of the node for which you want to view log events.
Domain, Service	Process	Process identification number for the Windows or UNIX service process that generated the log event. You can use the process identification number to identify log events from a process when an application service runs multiple processes on the same node.

Log Type	Option	Description
User Activity	Activity Code	Filter criteria for text that appears in the activity code. You can also use wildcards (*) in this text field.
User Activity	Activity	Filter criteria for text that appears in the activity. You can also use wildcards (*) in this text field.

- Click the Filter button.

The Log Manager retrieves the log events and displays them in the Logs tab with the most recent log events first.

- Click the Reset Filter button to view a different set of log events.

Tip: To search for logs related to an error or fatal log event, note the timestamp of the log event. Then, reset the filter and use a custom filter to search for log events during the timestamp of the event.

Configuring Log Columns

You can configure the Logs tab to display the following columns:

- Category
- Service Type
- Service Name
- Severity
- User
- Security Domain
- Timestamp
- Thread
- Message Code
- Message
- Node
- Process
- Activity Code
- Activity

Note: The columns appear based on the query options that you choose. For example, when you display a service type, the service name appears in the Logs tab.

- In the Administrator Tool, click the **Logs** tab.
- Select the **Domain**, **Service**, or **User Activity** view.
- To add a column, right-click a column name, select **Columns**, and then the name of the column you want to add.
- To remove a column, right-click a column name, select **Columns**, and then clear the checkmark next to the name of the column you want to remove.
- To move a column, select the column name, and then drag it to the location where you want it to appear.

The Log Manager updates the Logs tab columns with your selections.

Saving Log Events

You can save the log events that you filter and view in the Log Viewer. When you save log events, the Log Manager saves whatever logs that you are viewing based on the filter criteria. To save log events to a file, click Save Logs on the Log Actions menu.

The Log Manager does not delete the log events when you save them. The Administrator Tool prompts you to save or open the saved log events file.

Optionally, you can use the *infacmd* isp GetLog command to retrieve log events.

The format you choose to save log events to depends on how you plan to use the exported log events file:

- XML file. Use XML format if you want to analyze the log events in an external tool that uses XML or if you want to use XML tools, such as XSLT.
- Text file. Use a text file if you want to analyze the log events in a text editor.
- Binary file. Use binary format to back up the log events in binary format. You might need to use this format to send log events to Informatica Global Customer Support.

Exporting Log Events

You can export the log events to an XML, text, or binary file. To export log events to a file, click Export Logs on the Log Actions menu.

When you export log events, you can choose which logs you want to save. When you choose Service logs, you can export logs for a particular service type. You can choose the sort order of the log events in the export file.

The Log Manager does not delete the log events when you export them. The Administrator tool prompts you to save or open the exported log events file.

Optionally, you can use the *infacmd* GetLog command to retrieve log events.

The format you choose to export log events depends on how you plan to use the exported log events file:

- XML file. Use XML format if you want to analyze the log events in an external tool that uses XML or if you want to use XML tools, such as XSLT.
- Text file. Use a text file if you want to analyze the log events in a text editor.
- Binary file. Use binary format to back up the log events in binary format. You might need to use this format to send log events to Informatica Global Customer Support.

The following table describes the export log options for each log type:

Option	Log Type	Description
Type	Domain, Service, User Activity	Type of logs you want to export.
Service Type	Service	Type of application service for which to export log events. You can also export log events for all service types.

Option	Log Type	Description
Export Entries	Domain, Service, User Activity	Date range of log events you want to export. You can select the following options: <ul style="list-style-type: none"> - All Entries. Exports all log events. - Before Date. Exports log events that occurred before this date. Use the yyyy-mm-dd format when you enter a date. Optionally, you can use the calendar to choose the date. To use the calendar, click the date field.
Export logs in descending chronological order	Domain, Service, User Activity	Exports log events starting with the most recent log events.

XML Format

When you export log events to an XML file, the Log Manager exports each log event as a separate element in the XML file. The following example shows an excerpt from a log events XML file:

```
<log xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:common="http://
www.informatica.com/pcsf/common" xmlns:metadata="http://www.informatica.com/pcsf/
metadata" xmlns:domainservice="http://www.informatica.com/pcsf/domainservice"
xmlns:logservice="http://www.informatica.com/pcsf/logservice" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
<logEvent xsi:type="logservice:LogEvent" objVersion="1.0.0" timestamp="1129098642698"
severity="3" messageCode="AUTHEN_USER_LOGIN_SUCCEEDED" message="User Admin successfully
logged in." user="Admin" stacktrace="" service="authenticationservice"
serviceType="PCSF" clientNode="sapphire" pid="0" threadName="http-8080-Processor24"
context="" />
<logEvent xsi:type="logservice:LogEvent" objVersion="1.0.0" timestamp="1129098517000"
severity="3" messageCode="LM_36854" message="Connected to node [garnet] on outbound
connection [id = 2]." user="" stacktrace="" service="Copper" serviceType="IS"
clientNode="sapphire" pid="4484" threadName="4528" context="" />
```

Text Format

When you export log events to a text file, the Log Manager exports the log events in Information and Content Exchange (ICE) Protocol. The following example shows an excerpt from a log events text file:

```
2006-02-27 12:29:41 : INFO : (2628 | 2768) : (IS | Copper) : sapphire : LM_36522 :
Started process [pid = 2852] for task instance Session task instance
[s_DP_m_DP_AP_T_DISTRIBUTORS4]:Executor - Master.
2006-02-27 12:29:41 : INFO : (2628 | 2760) : (IS | Copper) : sapphire : CMN_1053 :
Starting process [Session task instance [s_DP_m_DP_AP_T_DISTRIBUTORS4]:Executor -
Master].
2006-02-27 12:29:36 : INFO : (2628 | 2760) : (IS | Copper) : sapphire : LM_36522 :
Started process [pid = 2632] for task instance Session task instance
[s_DP_m_DP_AP_T_DISTRIBUTORS4]:Preparer.
2006-02-27 12:29:35 : INFO : (2628 | 2760) : (IS | Copper) : sapphire : CMN_1053 :
Starting process [Session task instance [s_DP_m_DP_AP_T_DISTRIBUTORS4]:Preparer].
```

Binary Format

When you export log events to a binary file, the Log Manager exports the log events to a file that Informatica Global Customer Support can import. You cannot view the file unless you convert it to text. You can use the *infacmd* ConvertLogFile command to convert binary log files to text files, XML files, or readable text on the screen.

Viewing Administrator Tool Log Errors

If you receive an error while starting, updating, or removing services in the Administrator tool, an error message in the contents panel of the service provides a link to the Logs tab. Click the link in the error message to access detail information about the error in the Logs tab.

Log Events

The Service Manager and application services send log events to the Log Manager. The Log Manager generates log events for each service type.

You can view the following log event types on the Logs tab:

- Domain log events. Log events generated from the Service Manager functions.
- Analyst Service log events. Log events about each Analyst Service running in the domain.
- Content Management Service log events. Log events about each Content Management Service running in the domain.
- Data Integration Service log events. Log events about each Data Integration Service running in the domain.
- Metadata Manager Service log events. Log events about each Metadata Manager Service running in the domain.
- Model Repository log events. Log events about each Model Repository Service running in the domain.
- PowerCenter Integration Service log events. Log events about each PowerCenter Integration Service running in the domain.
- PowerCenter Repository Service log events. Log events from each PowerCenter Repository Service running in the domain.
- Reporting Service log events. Log events from each Reporting Service running in the domain.
- SAP BW Service log events. Log events about the interaction between the PowerCenter and the SAP NetWeaver BI system.
- Web Services Hub log events. Log events about the interaction between applications and the Web Services Hub.
- User activity log events. Log events about domain and security management tasks that a user completes.

Log Event Components

The Log Manager uses a common format to store and display log events. You can use the components of the log events to troubleshoot Informatica.

Each log event contains the following components:

- Service type, category, or user. The Logs tab categorizes events by domain category, service type, or user. If you view application service logs, the Logs tab displays the application service names. When you view domain logs, the Logs tab displays the domain categories in the log. When you view user activity logs, the Logs tab displays the users in the log.
- Message or activity. Message or activity text for the log event. Use the message text to get more information about the log events for domain and application services. Use the activity text to get more

information about log events for user activity. Some log events contain embedded log event in the message texts. For example, the following log events contains an embedded log event:

```
Client application [PmDTM], connection [59]: recv failed.
```

In this log event, the following log event is the embedded log event:

```
[PmDTM], connection [59]: recv failed.
```

When the Log Manager displays the log event, the Log Manager displays the severity level for the embedded log event.

- Security domain. When you view user activity logs, the Logs tab displays the security domain for each user.
- Message or activity code. Log event code. If the message type is error or fatal, click on the message code to open the Informatica Knowledge Base search for the message. You must configure the support portal credentials in the user account to do the search.
- Process. The process identification number for the Windows or UNIX service process that generated the log event. You can use the process identification number to identify log events from a process when an application service runs multiple processes on the same node.
- Node. Name of the node running the process that generated the log event.
- Thread. Identification number or name of a thread started by a service process.
- Time stamp. Date and time the log event occurred.
- Severity. The severity level for the log event. When you view log events, you can configure the Logs tab to display log events for a specific severity level.

Domain Log Events

Domain log events are log events generated from the domain functions the Service Manager performs. Use the domain log events to view information about the domain and troubleshoot issues. You can use the domain log events to troubleshoot issues related to the startup and initialization of nodes and application services for the domain.

Domain log events include log events from the following functions:

- Authorization. Log events that occur when the Service Manager authorizes user requests for services. Requests can come from the Administrator tool.
- Domain Configuration. Log events that occur when the Service Manager manages the domain configuration metadata.
- Node Configuration. Log events that occur as the Service Manager manages node configuration metadata in the domain.
- Licensing. Log events that occur when the Service Manager registers license information.
- License Usage. Log events that occur when the Service Manager verifies license information from application services.
- Log Manager. Log events from the Log Manager. The Log Manager runs on the master gateway node. It collects and processes log events for Service Manager domain operations and application services.
- Log Agent. Log events from the Log Agent. The Log Agent runs on all nodes in the domain. It retrieves PowerCenter workflow and session log events to display in the Workflow Monitor.
- Monitoring. Log events about Domain Functions.
- User Management. Log events that occur when the Service Manager manages users, groups, roles, and privileges.

- Service Manager. Log events from the Service Manager and signal exceptions from DTM processes. The Service Manager manages all domain operations. If the error severity level of a node is set to Debug, when a service starts the log events include the environment variables used by the service.

Analyst Service Log Events

Analyst Service log events contain the following information:

- Managing projects. Log events about managing projects in the Informatica Analyst, such as creating objects, folders, and projects. Log events about creating profiles, scorecards, and reference tables.
- Running jobs. Log events about running profiles and scorecards. Logs about previewing data.
- User permissions. Log events about managing user permissions on projects.

Data Integration Service Log Events

Data Integration Service logs contain logs about the following events:

- Configuration. Log events about system or service configuration changes, application deployment or removal, and logs about the associated profiling warehouse.
- Data Integration Service processes. Log events about application deployment, data object cache refresh, and user requests to run mappings, jobs, or workflows.
- System failures. Log events about failures that cause the Data Integration service to be unavailable, such as Model Repository connection failures or the service failure to start.

Listener Service Log Events

The PowerExchange Listener logs contain information about the application service that manages the PowerExchange Listener.

The Listener Service logs contain the following information:

- Client communication. Log events for communication between a PowerCenter or PowerExchange client and a data source.
- Listener service. Log events about the Listener service, including configuring, enabling, and disabling the service.
- Listener service operations. Log events for operations such as managing bulk data movement and change data capture.

Logger Service Log Events

The PowerExchange Logger Service writes logs about the application service that manages the PowerExchange Logger.

The Logger Service logs contain the following information:

- Connections. Log events about connections between the Logger Service and the source databases.
- Logger service. Log events about the Logger Service, including configuring, enabling, and disabling the service.
- Logger service operations. Log events for operations such as capturing changed data and writing the data to PowerExchange Logger files.

Model Repository Service Log Events

Model Repository Service log events contain the following information:

- Model Repository connections. Log events for connections to the repository from the Informatica Developer, Informatica Analyst, and Data Integration Service.
- Model Repository Service. Log events about Model Repository service, including enabling, disabling, starting, and stopping the service.
- Repository operations. Log events for repository operations such as creating and deleting repository content, and adding deployed applications.
- User permissions. Log events about managing user permissions on the repository.

Metadata Manager Service Log Events

The Metadata Manager Service log events contain information about each Metadata Manager Service running in the domain.

Metadata Manager Service log events contain the following information:

- Repository operations. Log events for accessing metadata in the Metadata Manager repository.
- Configuration. Log events about the configuration of the Metadata Manager Service.
- Run-time processes. Log events for running a Metadata Manager Service, such as missing native library files.
- PowerCenter Integration Service log events. Session and workflow status for sessions and workflows that use a PowerCenter Integration Service process to load data to the Metadata Manager warehouse or to extract source metadata.

To view log events about how the PowerCenter Integration Service processes a PowerCenter workflow to load data into the Metadata Manager warehouse, you must view the session or workflow log.

PowerCenter Integration Service Log Events

The PowerCenter Integration Service log events contain information about each PowerCenter Integration Service running in the domain.

PowerCenter Integration Service log events contain the following information:

- PowerCenter Integration Service processes. Log events about the PowerCenter Integration Service processes, including service ports, code page, operating mode, service name, and the associated repository and PowerCenter Repository Service status.
- Licensing. Log events for license verification for the PowerCenter Integration Service by the Service Manager.

PowerCenter Repository Service Log Events

The PowerCenter Repository Service log events contain information about each PowerCenter Repository Service running in the domain.

PowerCenter Repository Service log events contain the following information:

- PowerCenter Repository connections. Log events for connections to the repository from PowerCenter client applications, including user name and the host name and port number for the client application.

- PowerCenter Repository objects. Log events for repository objects locked, fetched, inserted, or updated by the PowerCenter Repository Service.
- PowerCenter Repository Service processes. Log events about PowerCenter Repository Service processes, including starting and stopping the PowerCenter Repository Service and information about repository databases used by the PowerCenter Repository Service processes. Also includes repository operating mode, the nodes where the PowerCenter Repository Service process runs, initialization information, and internal functions used.
- Repository operations. Log events for repository operations, including creating, deleting, restoring, and upgrading repository content, copying repository contents, and registering and unregistering local repositories.
- Licensing. Log events about PowerCenter Repository Service license verification.
- Security audit trails. Log events for changes to users, groups, and permissions. To include security audit trails in the PowerCenter Repository Service log events, you must enable the SecurityAuditTrail general property for the PowerCenter Repository Service in the Administrator tool.

Reporting Service Log Events

The Reporting Service log events contain information about each Reporting Service running in the domain.

Reporting Service log events contain the following information:

- Reporting Service processes. Log events about starting and stopping the Reporting Service.
- Repository operations. Log events for the Data Analyzer repository operations. This includes information on creating, deleting, backing up, restoring, and upgrading the repository content, and upgrading users and groups.
- Licensing. Log events about Reporting Service license verification.
- Configuration. Log events about the configuration of the Reporting Service.

SAP BW Service Log Events

The SAP BW Service log events contain information about the interaction between PowerCenter and the SAP NetWeaver BI system.

SAP NetWeaver BI log events contain the following log events for an SAP BW Service:

- SAP NetWeaver BI system log events. Requests from the SAP NetWeaver BI system to start a workflow and status information from the ZPMSENDSTATUS ABAP program in the process chain.
- PowerCenter Integration Service log events. Session and workflow status for sessions and workflows that use a PowerCenter Integration Service process to load data to or extract data from SAP NetWeaver BI.

To view log events about how the PowerCenter Integration Service processes an SAP NetWeaver BI workflow, you must view the session or workflow log.

Web Services Hub Log Events

The Web Services Hub log events contain information about the interaction between applications and the Web Services Hub.

Web Services Hub log events contain the following log events:

- Web Services processes. Log events about web service processes, including starting and stopping Web Services Hub, web services requests, the status of the requests, and error messages for web service calls. Log events include information about which service workflows are fetched from the repository.

- PowerCenter Integration Service log events. Workflow and session status for service workflows including invalid workflow errors.

User Activity Log Events

User activity log events describe all domain and security management tasks that a user completes. Use the user activity log events to determine when a user created, updated, or removed services, nodes, users, groups, or roles.

The Service Manager writes user activity log events when the Service Manager needs to authorize a user to perform one of the following domain actions:

- Enables or disables a service process.
- Starts, stops, enables, or disables a service.
- Adds, updates, or shuts down a node.
- Modifies the domain properties.
- Moves a folder in the domain.

The Service Manager also writes user activity log events each time a user performs the following security actions:

- Adds, updates, or removes a user, group, operating system profile, or role. The user activity log displays information about the user who performed the security action, but does not display the timestamp of the action.

The Service Manager also writes a user activity log event each time a user account is locked or unlocked.

Log Aggregator

You can aggregate the log files of an application service that stops responding or shuts down unexpectedly. You might need to analyze multiple log files to figure out issues with an application service.

You can use the log aggregator to aggregate all the log files associated with an application service and compress required log files into a .zip file. You can download the .zip file and analyze the log files, or upload the .zip file to Informatica Global Customer Support for analysis.

You cannot store the history of aggregated logs. You must download or send the file to Informatica Global Customer Support after you aggregate the log files.

You can aggregate the hang and crash logs of the following application services:

- Analyst Service
- Data Integration Service
- Model Repository Service
- PowerCenter Integration Service
- PowerCenter Repository Service

In addition to the application service logs, the log aggregator captures debug information for the nodes in the domain. The log aggregator aggregates the log files of the associated application services when you aggregate the log files of an application service. For example, when you aggregate the log files of an Analyst Service, the log aggregator aggregates the log files of the Data Integration Service and the Model Repository Service associated with the Analyst Service.

The log collection directory in the master gateway node stores the application service logs when you aggregate the logs. All the node processes in the domain must have read/write access on the log collection directory. If the node processes cannot access the log collection directory, the aggregated logs do not appear in the aggregated logs listgrid. The core dump directory stores the core dump files of the nodes in the domain. Configure the log collection directory in the master gateway node and the core dump directory for each node in the domain.

When you process the aggregated logs you can choose the collectors from which you want to collect log information. The collectors are application services and nodes associated with the application service.

Aggregating Application Service Logs

You can aggregate log files associated with hang or crash scenarios of an application service.

1. Click the **Logs** tab in the Administrator tool.
2. Click the **Log Aggregator** tab.
3. Select the application service for which you want to aggregate the logs.
4. Select the scenario for which you want to aggregate the logs.
You can choose between application service crash and hang scenarios.
5. Select the time interval to aggregate the logs.
You can choose to aggregate the logs from the previous 6 hours to 3 days.
6. Click **Next**.
7. Select the collectors from which you want to aggregate the logs.
The log aggregator displays the log files and the collectors based on the node to which they belong.
8. Click **Finish**.
The list of logs associated with the scenario appears in the right pane. You can download the aggregated logs or send the logs to the Informatica Global Customer Support.

Processing Aggregated Application Service Logs

After you aggregate the application service logs, you must download the aggregated zip file or send the logs to Informatica Global Customer Support.

Aggregate the application service logs based on your requirement.

1. Select the logs that you want to process.
2. Click **Actions > Compress Logs**.
The **Compressed Scenario Output** dialog box appears.
3. On the **Compressed Output** tab, click **Download** to download the aggregated log files as a zip file.
4. Optionally, click the **Send to Support** tab.
5. Enter the user name, password, and the TFTP directory of the Informatica My Support Portal.
6. Click **Send** to send the aggregated log files to Informatica Global Customer Support.

CHAPTER 11

Monitoring

This chapter includes the following topics:

- [Monitoring Overview, 173](#)
- [Monitoring Setup, 178](#)
- [Monitor Data Integration Services , 180](#)
- [Monitor Jobs, 181](#)
- [Monitor Applications, 182](#)
- [Monitor Deployed Mapping Jobs, 183](#)
- [Monitor Logical Data Objects, 184](#)
- [Monitor SQL Data Services, 185](#)
- [Monitor Web Services, 188](#)
- [Monitor Workflows, 189](#)
- [Monitoring a Folder of Objects, 198](#)
- [Monitoring an Object, 199](#)

Monitoring Overview

Monitoring is a domain function that the Service Manager performs. The Service Manager stores the monitoring configuration in the Model repository.

The Service Manager also persists, updates, retrieves, and publishes run-time statistics for integration objects in the Model repository. Integration objects include jobs, applications, logical data objects, SQL data services, web services, and workflows. Use the **Monitoring** tab in the Administrator tool to monitor integration objects that run on a Data Integration Service. The **Monitoring** tab shows properties, run-time statistics, and run-time reports about the integration objects. For example, the **Monitoring** tab can show the general properties and the status of a profiling job. It can also show the user who initiated the job and how long it took the job to complete. If you ran the a job on a grid, the Monitoring tab shows the nodes that ran the job. You can also view a graphical representation of the workflow in the Monitoring tool.

You can also access monitoring from the following locations:

Informatica Monitoring tool

You can access monitoring from the Informatica Monitoring tool. The Monitoring tool is a direct link to the **Monitoring** tab of the Administrator tool. The Monitoring tool is useful if you do not need access to any

other features in the Administrator tool. You must have at least one monitoring privilege to access the Monitoring tool. You can access the Monitoring tool by using the following URL:

```
http://<Administrator tool host> <Administrator tool port>/monitoring
```

Analyst tool

You can access monitoring from the Analyst tool. When you access monitoring from the Analyst tool, the monitoring results appear in the **Job Status** tab. The **Job Status** tab shows the status of Analyst tool jobs, such as profile jobs, scorecard jobs, and jobs that load mapping specification results to the target.

Developer tool

You can access monitoring from the Developer tool. When you access monitoring from the Developer tool, the monitoring results appear in the Informatica Monitoring tool. The Informatica Monitoring tool shows the status of Developer tool jobs, such as mapping jobs, web services, and SQL data services.

Navigator in the Monitoring Tab

Select an object in the Navigator of the **Monitoring** tab to monitor the object.

You can select the following types of objects in the Navigator in the **Monitoring** tab:

Data Integration Service

View general properties about the Data Integration Service, and view statistics about objects that run on the Data Integration Service.

Folder

View a list of objects contained in the folder. The folder is a logical grouping of objects. When you select a folder, a list of objects appears in the contents panel. The contents panel shows multiple columns that show properties about each object. You can configure the columns that appear in the contents panel.

The following table shows the folders that appear in the Navigator:

Folder	Location
Jobs	Appears under the Data Integration Service.
Deployed Mapping Jobs	Appears under the corresponding application.
Logical Data Objects	Appears under the corresponding application.
SQL Data Services	Appears under the corresponding application.
Web Services	Appears under the corresponding application.
Workflows	Appears under the corresponding application.

Integration objects

View information about the selected integration object. Integration objects include instances of applications, deployed mapping jobs, logical data objects, SQL data services, web services, and workflows.

Views in the Monitoring Tab

When you select an integration object in the Navigator or an object link in the contents panel of the **Monitoring** tab, multiple views of information appear in the contents panel. The views show information about the selected object, such as properties, run-time statistics, and run-time reports.

Depending on the type of object you select in the Navigator, the contents panel may display the following views:

Properties view

Shows general properties and run-time statistics about the selected object. General properties may include the name and description of the object. Statistics vary based on the selected object type.

Reports view

Shows reports for the selected object. The reports contain key metrics for the object. For example, you can view reports to determine the longest running jobs on a Data Integration Service during a particular time period.

Connections view

Shows connections defined for the selected object. You can view statistics about each connection, such as the number of closed, aborted, and total connections.

Requests view

Shows details about requests. There are two types of requests: SQL queries and Web Service requests. Users can use a third-party client tool to run SQL queries against the virtual tables in an SQL data service. Users can use a web service client to run Web Service requests against a web service. Each web service request runs a web service operation.

A request is a Web Services request or an SQL query that a user runs against a virtual table in an SQL data service.

Virtual Tables view

Shows virtual tables defined in an SQL data service. You can also view properties and cache refresh details for each virtual table.

Operations view

Shows the operations defined for the web service.

Statistics in the Monitoring Tab

The **Statistics** section in the **Properties** view shows aggregated statistics about the selected object. For example, when you select a Data Integration Service in the Navigator of the **Monitoring** tab, the **Statistics** section shows the total number of failed, aborted, completed, and canceled jobs that run on the selected Data Integration Service.

You can view statistics about the following integration objects:

Applications

Includes deployed mapping jobs, logical data objects, SQL data services, and web services.

Connections

Includes SQL connections to virtual databases.

Jobs

Includes jobs for profiles, previews, undeployed mappings, reference tables, and scorecards.

Requests

Includes SQL data service requests and web service requests.

Workflows

Includes workflow instances.

The following table describes the statistics for each object type:

Object Type	Statistics
Application Objects	<ul style="list-style-type: none">- Total. Total number of applications.- Running. Number of running applications.- Failed. Number of failed applications.- Stopped. Number of stopped applications.- Disabled. Number of disabled applications.
Connection Objects	<ul style="list-style-type: none">- Total. Total number of connections.- Closed. Number of closed connections. Closed connections are database connections on which SQL data service requests have previously run, but that are now closed. You cannot run requests against closed connections.- Aborted. Number of aborted connections. You chose to abort the connection, or the Data Integration Service was recycled or disabled in the abort mode when the connection was running.
Jobs	<ul style="list-style-type: none">- Total. Total number of jobs.- Failed. Number of failed jobs.- Aborted. Number of aborted jobs. The Data Integration Service was recycled or disabled in the abort mode when the job was running.- Completed. Number of completed jobs.- Canceled. Number of canceled jobs.
Request Objects	<ul style="list-style-type: none">- Total. Total number of requests.- Completed. Number of completed requests.- Aborted. Number of aborted requests. The Data Integration Service was recycled or disabled in the abort mode when the request was running.- Failed. Number of failed requests.
Workflows	<ul style="list-style-type: none">- Total. Total number of workflow instances.- Completed. Number of completed workflow instances.- Canceled. Number of canceled workflow instances.- Aborted. Number of aborted workflow instances.- Failed. Number of failed workflow instances.

Reports on the Monitoring Tab

You can view monitoring reports in the **Reports** view of the **Monitoring** tab. The **Reports** view appears when you select the appropriate object in the Navigator. You can view reports to monitor objects deployed to a Data Integration Service, such as jobs, web services, web service operations, SQL data services, and workflows.

The reports that appear in the **Reports view** are based on the selected object type and the reports configured to appear in the view. You must configure the monitoring preferences to enable reports to appear in the **Reports** view. By default, no reports appear in the **Reports** view.

You can view the following monitoring reports:

Longest Duration Jobs

Shows jobs that ran the longest during the specified time period. The report shows the job name, ID, type, state, and duration. You can view this report in the **Reports** view when you monitor a Data Integration Service in the **Monitoring** tab.

Longest Duration Mapping Jobs

Shows mapping jobs that ran the longest during the specified time period. The report shows the job name, state, ID, and duration. You can view this report in the **Reports** view when you monitor a Data Integration Service in the **Monitoring** tab.

Longest Duration Profile Jobs

Shows profile jobs that ran the longest during the specified time period. The report shows the job name, state, ID, and duration. You can view this report in the **Reports** view when you monitor a Data Integration Service in the **Monitoring** tab.

Longest Duration Reference Table Jobs

Shows reference table process jobs that ran the longest during the specified time period. Reference table jobs are jobs where you export or import reference table data. The report shows the job name, state, ID, and duration. You can view this report in the **Reports** view when you monitor a Data Integration Service in the **Monitoring** tab.

Longest Duration Scorecard Jobs

Shows scorecard jobs that ran the longest during the specified time period. The report shows the job name, state, ID, and duration. You can view this report in the **Reports** view when you monitor a Data Integration Service in the **Monitoring** tab.

Longest Duration SQL Data Service Connections

Shows SQL data service connections that were open the longest during the specified time period. The report shows the connection ID, SQL data service, connection state, and duration. You can view this report in the **Reports** view when you monitor a Data Integration Service, an SQL data service, or an application in the **Monitoring** tab.

Longest Duration SQL Data Service Requests

Shows SQL data service requests that ran the longest during the specified time period. The report shows the request ID, SQL data service, request state, and duration. You can view this report in the **Reports** view when you monitor a Data Integration Service, an SQL data service, or an application in the **Monitoring** tab.

Longest Duration Web Service Requests

Shows web service requests that were open the longest during the specified time period. The report shows the request ID, web service operation, request state, and duration. You can view this report in the **Reports** view when you monitor a Data Integration Service, a web service, or an application in the **Monitoring** tab.

Longest Duration Workflows

Shows all workflows that were running the longest during the specified time period. The report shows the workflow name, state, instance ID, and duration. You can view this report in the **Reports** view when you monitor a Data Integration Service or an application in the **Monitoring** tab.

Longest Duration Workflows Excluding Human Tasks

Shows workflows that do not include a Human task that were running the longest during the specified time period. The report shows the workflow name, state, instance ID, and duration. You can view this report in the **Reports** view when you monitor a Data Integration Service or an application in the **Monitoring** tab.

Minimum, Maximum, and Average Duration Report

Shows the total number of SQL data service and web service requests during the specified time period. Also shows the minimum, maximum, and average duration for the requests during the specified time period. The report shows the object type, total number of requests, minimum duration, maximum duration, and average duration. You can view this report in the **Reports** view when you monitor a Data Integration Service, an SQL data service, a web service, or an application in the **Monitoring** tab.

Most Active IP for SQL Data Service Requests

Shows the total number of SQL data service requests from each IP address during the specified time period. The report shows the IP address and total requests. You can view this report in the **Reports** view when you monitor a Data Integration Service, an SQL data service, or an application in the **Monitoring** tab.

Most Active SQL Data Service Connections

Shows SQL data service connections that received the most connection requests during the specified time period. The report shows the connection ID, SQL data service, and the total number of connection requests. You can view this report in the **Reports** view when you monitor a Data Integration Service, an application, or an SQL data service in the **Monitoring** tab.

Most Active Users for Jobs

Shows users that ran the most number of jobs during the specified time period. The report shows the user name and the total number of jobs that the user ran. You can view this report in the **Reports** view when you monitor a Data Integration Service in the **Monitoring** tab.

Most Active Web Service Client IP

Shows IP addresses that received the most number of web service requests during the specified time period. The report shows the IP address and the total number of requests. You can view this report in the **Reports** view when you monitor a Data Integration Service, an application, a web service, or web service operation in the **Monitoring** tab.

Most Frequent Errors for Jobs

Shows the most frequent errors for jobs, regardless of job type, during the specified time period. The report shows the job type, error ID, and error count. You can view this report in the **Reports** view when you monitor a Data Integration Service in the **Monitoring** tab.

Most Frequent Errors for SQL Data Service Requests

Shows the most frequent errors for SQL data service requests during the specified time period. The report shows the error ID and error count. You can view this report in the **Reports** view when you monitor a Data Integration Service, an SQL data service, or an application in the **Monitoring** tab.

Most Frequent Faults for Web Service Requests

Shows the most frequent faults for web service requests during the specified time period. The report shows the fault ID and fault count. You can view this report in the **Reports** view when you monitor a Data Integration Service, a web service, or an application in the **Monitoring** tab.

Monitoring Setup

You configure the domain to set up monitoring. When you set up monitoring, the Data Integration Service stores persisted statistics and monitoring reports in a Model repository. Persisted statistics are historical

information about integration objects that previously ran. The monitoring reports show key metrics about an integration object.

Complete the following tasks to enable and view statistics and monitoring reports:

1. Configure the global settings for the Data Integration Service.
2. Configure preferences for statistics and reports.

Step 1. Configure Global Settings

Configure global settings for the domain to specify the Model repository that stores the run-time statistics about objects deployed to Data Integration Services. The global settings apply to all Data Integration Services defined in the domain. If you do not configure the global settings, the workflow graph will be empty and the notifications disappear when you refresh the page.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, select the domain.
3. In the contents panel, click **Actions > Global Settings**.
4. Edit the following options:

Option	Description
Model Repository Service	Name of the Model Repository Service that stores the historical information.
Username	User name for the Model Repository Service.
Password	Password for the Model Repository Service.
Number of Days to Preserve Historical Data	Number of days that the Data Integration Service stores historical run-time statistics. Set to '0' if you do not want the Data Integration Service to preserve historical run-time statistics.
Purge Statistics Every	Frequency, in days, at which the Data Integration Service purges statistics. Default is 1.
Days At	Time of day when the Data Integration Service purges old statistics. Default is 1:00 a.m.
Maximum Number of Sortable Records	Maximum number of records that can be sorted in the Monitoring tab. If the number of records that appear on the Monitoring tab is greater than this value, you can sort only on the Start Time and End Time columns. Default is 3,000.
Maximum Delay for Update Notifications	Maximum time period, in seconds, that the Data Integration Service buffers the statistics before persisting the statistics in the Model repository and displaying them in the Monitoring tab. If the Data Integration Service shuts down unexpectedly before the service persists the statistics in the Model repository, the statistics are lost. Default is 10.
Show Milliseconds	Include milliseconds for date and time fields in the Monitoring tab.

Note: If you enable Kerberos security in the domain, the Username and Password fields do not appear.

5. Click **OK**.
6. Click **Save** to save the global settings.

Restart all Data Integration Services in the domain to apply the settings.

Step 2. Configure Monitoring Preferences

You must configure the time ranges for statistics and reports for the domain. These settings apply to all Data Integration Services. You also can configure the reports that appear in the **Monitoring** tab.

You must specify a Model Repository Service in the global settings, and the Model Repository Service must be available before you can configure the preferences.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, select the domain.
3. In the contents panel, click **Actions > Preferences**.
4. Click the **Statistics** tab.
5. Configure the time ranges that you want to use for statistics, and then select the frequency at which the statistics assigned to each time range should be updated.
6. Select a default time range to appear for all statistics.
7. Click the **Reports** tab.
8. Enable the time ranges that you want to use for reports, and then select the frequency at which the reports assigned to each time range should be updated.
9. Select a default time range to appear for all reports, and then click **OK**.
10. Click **Select Reports**.
11. Add the reports that you want to run to the **Selected Reports** box.
12. Organize the reports in the order in which you want to view them on the **Monitoring** tab.
13. Click **OK** to close the **Select Reports** window.
14. Click **OK** to close the **Preferences** window.
15. Click **Save** to save the preferences.

Monitor Data Integration Services

You can monitor Data Integration Services on the **Monitoring** tab.

When you select a Data Integration Service in the Navigator of the **Monitoring** tab, the contents panel shows the following views:

- **Properties** view
- **Reports** view

Properties View for a Data Integration Service

The **Properties** view shows the general properties and run-time statistics for objects that ran on the selected Data Integration Service.

When you select a Data Integration Service in the Navigator, you can view the general properties and run-time statistics.

General Properties for a Data Integration Service

You can view general properties, such as the service name, object type, and description. The **Persist Statistics Enabled** property indicates whether the Data Integration Service stores persisted statistics in the Model repository. This option is true when you configure the global settings for the domain.

You can also view information about objects that run on the Data Integration Service. To view information about an object, select the object in the Navigator or contents panel. Depending on the object type, details about the object appear in the contents panel or details panel.

Statistics for a Data Integration Service

You can view run-time statistics about objects that run on the Data Integration Service. Select the object type and time period to display the statistics. You can view statistics about jobs, applications, connections, requests, and workflows. For example, you can view the number of failed, canceled, and completed profiling jobs in the last four hours.

Reports View for a Data Integration Service

The **Reports** view shows monitoring reports about objects that run on the selected Data Integration Service.

When you monitor a Data Integration Service in the **Monitoring** tab, the **Reports** view shows reports about jobs, SQL data services, web services, and workflows. For example, you can view the Most Active Users for Jobs report to determine users that ran the most jobs during a specific time period. Click a link in the report to show more details about the objects included in the link. For example, you can click the number of failed deployed mappings to see details about each deployed mapping that failed.

Monitor Jobs

You can monitor Data Integration Service jobs on the **Monitoring** tab. A job is a preview, scorecard, profile, mapping, or reference table process that runs on a Data Integration Service. Reference table jobs are jobs where you export or import reference table data.

When you select **Jobs** in the Navigator of the **Monitoring** tab, a list of jobs appears in the contents panel. The contents panel groups related jobs based on the job type. You can expand a job type to view the related jobs under it.

For example, when you run a profile job on a grid, the Data Integration Service splits the work into multiple mappings. The mappings appear under the profile job in the contents panel. The contents panel also shows the node that runs each mapping of the profile.

By default, you can view jobs that you created. If you have the appropriate monitoring privilege, you can view jobs of other users. You can view properties about each job in the contents panel. You can also view logs, view the context of jobs, and cancel jobs.

You run jobs from the Developer tool. The Developer tool can run up to five jobs at a time. All remaining jobs are queued. The Administrator tool shows Developer tool jobs that are currently running. It does not show jobs that are queued in the Developer tool.

When you select a job in the contents panel, job properties for the selected job appear in the details panel. Depending on the type of job, the details panel may show general properties and mapping properties.

General Properties for a Job

The details panel shows the general properties about the selected job, such as the name, job type, user who started the job, and start time of the job. If you ran the job on a grid, the details panel also shows the node that ran the job.

Mapping Properties for a Job

The **Mapping** section appears in the details panel when you select a profile or scorecard job in the contents panel. These jobs have an associated mapping. You can view mapping properties such as the request ID, the mapping name, and the log file name.

Viewing Logs for a Job

You can download the logs for a job to view the job details.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service and select **Jobs**.
3. In the contents panel, select a job.
4. Click **Actions > View Logs for Selected Object**.

A dialog box appears with the option to open or save the log file.

Canceling a Job

You can cancel a running job. You may want to cancel a job that hangs or that is taking an excessive amount of time to complete.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service and select **Jobs**.
3. In the contents panel, select a job.
4. Click **Actions > Cancel Selected Object**.

Monitor Applications

You can monitor applications on the **Monitoring** tab.

When you select an application in the Navigator of the **Monitoring** tab, the contents panel shows the following views:

- **Properties** view
- **Reports** view

You can expand an application in the Navigator to monitor the objects in the application, such as deployed mapping jobs, logical data objects, SQL data services, web services, and workflows.

Properties View for an Application

The **Properties** view shows general properties and run-time statistics about each application and the objects in an application. Applications can include deployed mapping jobs, logical data objects, SQL data services, web services, and workflows.

When you select an application in the contents panel of the **Properties** view, you can view the general properties and run-time statistics.

General Properties for an Application

You can view general properties, such as the name and description of the application. You can also view additional information about the objects in an application. To view information about an object, select the folder in the Navigator and the object in the contents panel. The object appears under the application in the Navigator. Details about the object appear in the details panel.

Statistics for an Application

You can view run-time statistics about an application and about the jobs, connections, requests, and workflows associated with the application. For example, you can view the number of enabled and disabled applications, number of aborted connections, and number of completed, failed, and canceled jobs and workflows.

Reports View for an Application

The **Reports** view shows monitoring reports about the selected application.

When you monitor an application in the **Monitoring** tab, the **Reports** view shows reports about objects contained in the application. For example, you can view the Most Active WebService Client IP report to determine the IP addresses that received the most number of web service requests during a specific time period.

Monitor Deployed Mapping Jobs

You can monitor deployed mapping jobs on the **Monitoring** tab.

You can view information about deployed mapping jobs in an application. When you select **Deployed Mapping Jobs** under an application in the Navigator of the **Monitoring** tab, a list of deployed mapping jobs appears in the contents panel. The contents panel shows properties about each deployed mapping job, such as Job ID, name of mapping, state of the job, and start time of the job. If you ran the job on a grid, the contents panel also shows the node that ran the job.

Select a deployed mapping job in the contents panel to view logs for the job, reissue the job, and cancel the job.

When you select the link for a deployed mapping job in the contents panel, the contents panel shows the **Mapping Properties** view. The view shows mapping properties such as the request ID, the mapping name, and the log file name.

Viewing Logs for a Deployed Mapping Job

You can download the logs for a deployed mapping job to view the job details.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **Deployed Mapping Jobs**.

A list of mapping jobs appear in the contents panel.

4. In the contents panel, select a mapping job.
5. Click **Actions > View Logs for Selected Object**.

A dialog box appears with the option to open or save the log file.

Reissuing a Deployed Mapping Job

You can reissue a deployed mapping job when the mapping jobs fails. When you reissue a deployed mapping job, the Data Integration Service runs the job again.

1. In the Administrator tool, click the **Monitoring** tab.

2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **Deployed Mapping Jobs**.
The contents panel displays a list of deployed mapping jobs.
4. In the contents panel, select a deployed mapping job.
5. Click **Actions > Reissue Selected Object**.

Canceling a Deployed Mapping Job

You can cancel a deployed mapping job. You may want to cancel a deployed mapping job that hangs or that is taking an excessive amount of time to complete.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **Deployed Mapping Jobs**.
The contents panel displays a list of deployed mapping jobs.
4. In the contents panel, select a deployed mapping job.
5. Click **Actions > Cancel Selected Job**.

Monitor Logical Data Objects

You can monitor logical data objects on the **Monitoring** tab.

You can view information about logical data objects included in an application. When you select **Logical Data Objects** under an application in the Navigator of the **Monitoring** tab, a list of logical data objects appears in the contents panel. The contents panel shows properties about each logical data object.

Select a logical data object in the contents panel to download the logs for a data object.

When you select the link for a logical data object in the contents panel, the details panel shows the following views:

- **Properties** view
- **Cache Refresh Runs** view

Properties View for a Logical Data Object

The **Properties** view shows general properties and run-time statistics about the selected object.

You can view properties such as the data object name, logical data object model, folder path, cache state, and last cache refresh information.

Cache Refresh Runs View for a Logical Data Object

The **Cache Refresh Runs** view shows cache refresh details about the selected logical data object.

The **Cache Refresh Runs** view shows cache refresh details such as the cache run ID, request count, and row count.

Viewing Logs for Data Object Cache Refresh Runs

You can download the logs for data object cache refresh runs to view the cache refresh run details.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **Logical Data Objects**.

The contents panel displays a list of logical data objects.

4. In the contents panel, select a logical data object.
Details about the selected data object appear in the details panel.
5. In the details panel, select the **Cache Refresh Runs** view.
6. In the details panel, click **View Logs for Selected Object**.

Monitor SQL Data Services

You can monitor SQL data services on the **Monitoring** tab. An SQL data service is a virtual database that you can query. It contains a schema and other objects that represent underlying physical data.

You can view information about the SQL data services included in an application. When you select **SQL Data Services** under an application in the Navigator of the **Monitoring** tab, a list of SQL data services appears in the contents panel. The contents panel shows properties about each SQL data service, such as the name, description, and state.

When you select the link for a SQL data service in the contents panel, the contents panel shows the following views:

- **Properties** view
- **Connections** view
- **Requests** view
- **Virtual Tables** view
- **Reports** view

Properties View for an SQL Data Service

The **Properties** view shows general properties and run-time statistics for an SQL data service.

When you select an SQL data service in the contents panel of the **Properties** view, you can view the general properties and run-time statistics.

General Properties for an SQL Data Service

You can view general properties, such as the SQL data service name and the description.

Statistics for an SQL Data Service

You can view run-time statistics about connections and requests for the SQL data service. Sample statistics include the number of connections to the SQL data service, the number of requests, and the number of aborted connections.

Connections View for an SQL Data Service

The **Connections** view displays properties about connections from third-party clients. The view shows properties such as the connection ID, state of the connection, connect time, elapsed time, and disconnect time.

When you select a connection in the contents panel, you can abort the connection or access the **Properties** view and **Requests** view in the details panel.

Properties View

The **Properties** view in the details panel shows the user who is using the connection, the state of the connection, and the connect time.

Requests View

The **Requests** view in the details panel shows information about the requests for the SQL connection. Each connection can have more than one request. The view shows request properties such as request ID, user name, state of the request, start time, elapsed time, and end time.

Aborting a Connection

You can abort a connection to prevent it from sending more requests to the SQL data service.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **SQL Data Services**.
The contents panel displays a list of SQL data services.
4. In the contents panel, select an SQL data service.
The contents panel displays multiple views for the SQL data service.
5. In the contents panel, click the **Connections** view.
The contents panel lists connections to the SQL data service.
6. Select a connection.
7. Click **Actions > Abort Selected Connection**.

Requests View for an SQL Data Service

The **Requests** view displays properties for requests for each SQL connection.

The **Requests** view shows properties about the requests for the SQL connection. Each connection can have more than one request. The view shows request properties such as request ID, connection ID, user name, state of the request, start time, elapsed time, and end time.

Select a request in the contents panel to view additional information about the request in the details panel.

Aborting an SQL Data Service Connection Request

You can abort an SQL Data Service connection request. You might want to abort a connection request that hangs or that is taking an excessive amount of time to complete.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **SQL Data Services**.
The contents panel displays a list of SQL data services.

4. In the contents panel, select an SQL data service.
5. In the contents panel, click the **Requests** view.
A list of connection requests for the SQL data service appear.
6. In the contents panel, select a request row.
7. Click **Actions > Abort Selected Request**.

Viewing Logs for an SQL Data Service Request

You can download the logs for an SQL data service request to view the request details.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **SQL Data Services**.
The contents panel displays a list of SQL data services.
4. In the contents panel, select an SQL data service.
5. In the contents panel, click the **Requests** view.
A list of requests for the SQL data service appear.
6. In the contents panel, select a request row.
7. Click **Actions > View Logs for Selected Object**.

Virtual Tables View for an SQL Data Service

The **Virtual Tables** view displays properties about the virtual tables in the SQL data service.

The view shows properties about the virtual tables, such as the name and description. When you select a virtual table in the contents panel, you can view the **Properties** view and **Cache Refresh Runs** view in the details panel.

Properties View

The **Properties** view displays general information and run-time statistics about the selected virtual table. General properties include the virtual table name and the schema name. Monitoring statistics include the number of request, the number of rows cached, and the last cache refresh time.

Cache Refresh Runs View

The **Cache Refresh Runs** view displays cache information for the selected virtual table. The view includes the cache run ID, the request count, row count, and the cache hit rate. The cache hit rate is the total number of requests on the cache divided by the total number of requests for the data object.

Viewing Logs for an SQL Data Service Table Cache

You can download the logs for an SQL data service table cache to view the table cache details.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **SQL Data Services**.
The contents panel displays a list of SQL data services.
4. In the contents panel, select an SQL data service.
5. In the contents panel, click the **Virtual Tables** view.

A list of virtual tables for the SQL data service appear.

6. In the contents panel, select a table row.

Details about the selected table appear in the details panel.

7. In the details panel, select the **Cache Refresh Runs** view.
8. In the details panel, click **View Logs for Selected Object**.

Reports View for an SQL Data Service

The **Reports** view shows monitoring reports about the selected SQL data service.

When you monitor an SQL data service in the **Monitoring** tab, the **Reports** view shows reports about the SQL data service. For example, you can view the Most Active SQL Connections report to determine the SQL connections that received the most connection requests during a specific time period.

Monitor Web Services

You can monitor web services on the **Monitoring** tab. Web services are business functions that operate over the Web. They describe a collection of operations that are network accessible through standardized XML messaging.

You can view information about web services included in an application. When you select **Web Services** under an application in the Navigator of the **Monitoring** tab, a list of web services appears in the contents panel. The contents panel shows properties about each web service, such as the name, description, and state of each web service.

When you select the link for a web service in the contents panel, the contents panel shows the following views:

- **Properties** view
- **Reports** view
- **Operations** view
- **Requests** view

Properties View for a Web Service

The **Properties** view shows general properties and run-time statistics for a web service.

When you select a web service in the contents panel of the **Properties** view, you can view the general properties and monitoring statistics.

General Properties for a Web Service

You can view general properties about the web service, such as the name and type of object.

Statistics for a Web Service

You can view run-time statistics about web service requests during a specific time period. The **Statistics** section shows the number of completed, failed, and total web service requests.

Reports View for a Web Service

The **Reports** view shows monitoring reports about the selected web service.

When you monitor a web service in the **Monitoring** tab, the **Reports** view shows reports about the web service. For example, you can view the Most Active WebService Client IP report to determine the IP addresses that received the most number of web service requests during a specific time period.

Operations View for a Web Service

The **Operations** view shows the name and description of each operation included in the web service. The view also displays properties, requests, and reports about each operation.

When you select a web service operation in the contents panel, the details panel shows the **Properties** view, **Requests** view, and **Reports** view.

Properties View for a Web Service Operation

The **Properties** view shows general properties and statistics about the selected web service operation. General properties include the operation name and type of object. The view also shows statistics about the web service operation during a particular time period. Statistics include the number of completed, failed, and total web service requests.

Requests View for a Web Service Operation

The **Requests** view shows properties about each web service operation, such as request ID, user name, state, start time, elapsed time, and end time. You can filter the list of requests. You can also view logs for the selected web service request.

Reports View for a Web Service Operation

The **Reports** view shows reports about web service operations.

Requests View for a Web Service

The **Requests** view shows properties about each web service request, such as request ID, user name, state, start time, elapsed time, and end time. You can filter the list of requests.

When you select a web service request in the contents panel, you can view logs about the request in the details panel. The details panel shows general properties and statistics about the selected web service request. Statistics include the number of completed, failed, and total web service requests.

You can also abort a web service request from the **Requests** view. To abort a web service request, select the workflow request and click **Actions > Abort Selected Request** in the contents panel.

Monitor Workflows

You can monitor workflows on the **Monitoring** tab.

You can view information about workflow instances that are run from a workflow in a deployed application. When you select **Workflows** under an application in the Navigator of the **Monitoring** tab, a list of workflow instances appears in the contents panel. The contents panel shows properties about each workflow instance, such as the name, state, start time, and recovery properties of each workflow instance. If you ran a workflow instance on a grid, the contents panel also shows the node that ran each mapping in the workflow instance.

Select a workflow instance in the contents panel to perform the following tasks:

- View logs for the workflow instance.
- View the context of the workflow instance to view other workflow instances that started around the same time as the selected workflow instance.
- Cancel or abort the workflow instance.
- Recover the interrupted workflow instance.

Expand a workflow instance to view properties about each workflow object, including tasks and gateways.

Workflow Graph

You can view the details of a workflow that you run in the Monitoring tool in a graphical form.

After you run a workflow, you can see the graphical view of the workflow in the Monitoring tool. In the workflow graph, you can see the sequential run of the mapping tasks in the workflow. The workflow graph enables you to view the failure points in a workflow at a glance.

In the workflow graph, you can view the following details of a workflow:

- Mapping tasks in the workflow
- Task details
- Recovery details

You can perform the following tasks from the workflow graph:

- Abort a running workflow
- Cancel a running workflow
- Recover a failed workflow
- View the workflow logs

Viewing Workflow Graph

You can view the graphical view of a workflow from the monitoring tool.

1. Click on the Monitoring tab in the Administrator tool.
2. Expand the project that contains the workflow that you want to view in the Navigator.
3. Select the workflow that you want to view.
4. Click **Actions > View Workflow Graph**.

The workflow graph for the workflow appears in a new window.

View Workflow Objects

When you expand a workflow instance in the contents panel, you can view properties about workflow objects, such as the name, state, start time, and elapsed time for the object.

Workflow objects include events, tasks, and gateways. When you monitor workflows, you can also monitor the tasks and gateways that run in a workflow instance. The Monitoring tab does not display information about events in the workflow instance.

If an expression in a conditional sequence flow evaluates to false, the Data Integration Service does not run the next object or any of the subsequent objects in that branch. The Monitoring tab does not list objects that do not run in the workflow instance. When a workflow instance includes objects that do not run, the instance can still successfully complete.

You can expand a task in the contents panel to view information about the work item run by the task. For example, expand a Mapping task to view information about the mapping run by the Mapping task.

Workflow States

When you monitor a workflow instance, you can view the state of the workflow instance. If the workflow instance encounters the state during a recovery run, the state has the text (Recovery) appended to it.

A workflow instance can have one of the following states:

Aborted

A workflow instance aborts in the following situations:

- The workflow is enabled for recovery and a task with a restart recovery strategy encounters a recoverable error.
- You choose to abort the workflow instance from the Monitoring tool or using the `infacmd wfs abortWorkflow` command. You can also choose to abort a running workflow instance when you disable or recycle the Data Integration Service, when you stop the application that contains the workflow, or when you disable the workflow in the application.
- The workflow is enabled for recovery and the Data Integration Service process shuts down unexpectedly while running this workflow instance.

While the Data Integration Service process remains in a disabled state after shutting down, the workflow instance state remains Running although the instance is no longer running. If the workflow is not configured for automatic recovery, the service process changes the workflow instance state to Aborted when the service process restarts. If the workflow is configured for automatic recovery, the service process recovers the workflow instance when the service process restarts. The service changes the workflow instance state to Running (Recovery).

Canceled

You choose to cancel the workflow instance from the Monitoring tab or by using the `infacmd wfs cancelWorkflow` command.

Completed

The Data Integration Service successfully completes the workflow instance. A completed workflow instance means that all tasks, gateways, and sequence flow evaluations either successfully completed or were in a branch that did not run.

Failed

A workflow instance fails in the following situations:

- A workflow error occurred. Workflow errors can occur when the Data Integration Service reads the parameter file at the start of the workflow run, copies workflow parameter and variable values to task input, or evaluates expressions in conditional sequence flows. In addition, a workflow error occurs if an Assignment task or an Exclusive gateway fails.

When a workflow error occurs, the Data Integration Service stops processing additional objects and fails the workflow instance immediately.

- A Command, Mapping, Notification, or Human task in the workflow instance failed.

When these tasks fail, the Data Integration Service continues to run additional objects in the workflow instance if expressions in the conditional sequence flows evaluate to true or if the sequence flows do not include conditions. If the workflow instance finishes running without another interruption, the Data Integration Service updates the workflow state to Failed. A failed workflow instance can contain both failed and completed tasks.

Running

The Data Integration Service is running the workflow instance.

Unknown

A workflow instance has an Unknown state in the following situations:

- The workflow is not enabled for recovery and the Data Integration Service process shuts down unexpectedly while running this workflow instance.

While the Data Integration Service process remains in a disabled state, the workflow instance state remains Running although the instance is no longer running. When the service process restarts, the service changes the workflow instance state to Unknown.

- The workflow is enabled for recovery and the workflow instance has an aborted or canceled state. You change the workflow definition in the Developer tool and redeploy the application that contains the workflow. Because the workflow metadata has changed, the workflow instance is no longer recoverable. As a result, the Data Integration Service updates the state of the workflow instance to Unknown.
- You choose to abort a running workflow instance when you disable or recycle the Data Integration Service, when you stop the application that contains the workflow, or when you disable the workflow in the application. The Data Integration Service attempts to kill the process on any running task for 60 seconds. If the service cannot abort the running task in 60 seconds, the service shuts down the workflow instance and updates the workflow instance state to Unknown.

Workflow Object States

When you monitor a workflow instance, you can view the state of all tasks and gateways that run in the workflow instance. If the task or gateway encounters the state during a recovery run, the state has the text (Recovery) appended to it.

Tasks and gateways can have one of the following states:

Aborted

Tasks and gateways can abort for multiple reasons.

The following table describes the reasons that can cause tasks and gateways to abort:

Reason for the Abort	Task and Gateway Type	Description
You choose to abort the workflow instance.	Command Mapping Notification	<p>A task aborts in the following situations:</p> <ul style="list-style-type: none"> - The task is in a workflow not enabled for recovery and is running when you choose to abort the workflow instance. - The task has a restart recovery strategy in a workflow enabled for recovery and is running when you choose to abort the workflow instance. <p>After the task aborts, the Data Integration Service aborts the workflow instance.</p> <p>If you choose to abort the workflow instance while an Assignment task or gateway is running, the Data Integration Service completes running the task or gateway. The service then aborts the workflow instance and does not start running any additional objects.</p>
Task with a restart recovery strategy encounters a recoverable error.	Command Mapping Notification	The task has a restart recovery strategy in a workflow enabled for recovery and the task encounters a recoverable error.
Service process shuts down unexpectedly.	All task types Exclusive gateway	<p>A task with a restart recovery strategy, an Assignment task, or an Exclusive gateway is in a workflow enabled for recovery. The task or gateway is running when the Data Integration Service process shuts down unexpectedly.</p> <p>While the Data Integration Service process remains in a disabled state, the task state remains Running although the task is no longer running.</p> <p>If the workflow is not configured for automatic recovery, the service process changes the task state to Aborted when the service process restarts.</p> <p>If the workflow is configured for automatic recovery, the service process recovers the workflow instance and restarts the interrupted task when the service process restarts. The service process changes the task state to Running (Recovery).</p>

Completed

The Data Integration Service successfully completes the task or gateway.

Failed

A task or gateway fails in the following situations:

- Any task or gateway in a workflow not enabled for recovery encounters any type of error.
- An Assignment task or an Exclusive gateway in a workflow enabled for recovery encounters any type of error.
- A Command, Mapping, or Notification task with a restart recovery strategy in a workflow enabled for recovery encounters a non recoverable error.
- A Command, Mapping, or Notification task with a skip recovery strategy in a workflow enabled for recovery encounters any type of error, is running when the workflow instance aborts, or is running when the service process shuts down unexpectedly.

Running

The Data Integration Service is running the task or gateway.

Unknown

A task or gateway has an Unknown state in the following situations:

- A task or gateway is in a workflow not enabled for recovery. The task or gateway is running when the Data Integration Service process shuts down unexpectedly.

While the Data Integration Service process remains in a disabled state, the task or gateway state remains Running although the task or gateway is no longer running. When the service process restarts, the service changes the task or gateway state to Unknown.

- You choose to abort a running workflow instance when you disable or recycle the Data Integration Service, when you stop the application that contains the workflow, or when you disable the workflow in the application. The Data Integration Service attempts to kill the process on any running task or gateway for 60 seconds. If the service cannot abort the running task or gateway in 60 seconds, the service shuts down the workflow instance and updates the task or gateway state to Unknown.

Mapping Task Work Item States

When you expand a Mapping task, you can view the state of the mapping run. When you expand a restarted Mapping task, you can view the mapping jobs run for each recovery attempt of the workflow instance.

If the Mapping task encounters the state during a recovery run, the state has the text (Recovery) appended to it. You can also view the state of the mapping run from the workflow graph of the workflow that contains the mapping task.

Mappings run by a Mapping task can have one of the following states:

Aborted

The Mapping task aborts while the mapping is running because you choose to abort the workflow instance.

Completed

The Data Integration Service successfully completes the mapping.

Failed

The mapping encounters an error. If the Mapping task has a restart recovery strategy in a workflow enabled for recovery and the mapping encounters an error, the mapping fails but the Mapping task aborts.

Running

The Data Integration Service is running the mapping.

Unknown

The Mapping task is in a workflow that is enabled for recovery or is not enabled for recovery. The mapping is running when the Data Integration Service process shuts down unexpectedly.

While the Data Integration Service process remains in a disabled state, the mapping state remains Running although the mapping is no longer running. When the service process restarts, the service changes the mapping state to Unknown.

Canceling or Aborting a Workflow

You can cancel or abort a workflow instance at anytime. You might want to cancel or abort a workflow instance that stops responding or that is taking an excessive amount of time to complete.

When you cancel a workflow instance, the Data Integration Service finishes processing any running task and then stops processing the workflow instance. The service does not start running any subsequent workflow objects.

When you abort a workflow instance, the Data Integration Service attempts to kill the process on any running task. If an Assignment task or an Exclusive gateway is running, the Data Integration Service completes the task or gateway. After the task aborts or completes, the service aborts the workflow instance. The service does not start running any subsequent workflow objects.

You can also cancel or abort a workflow from the workflow graph.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **Workflows**.
A list of workflow instances appear in the contents panel.
4. In the contents panel, select a workflow instance.
5. Click **Actions > Cancel Selected Workflow** or **Actions > Abort Selected Workflow**.

Workflow Recovery

Workflow recovery is the completion of a workflow instance from the point of interruption.

When a workflow is enabled for recovery, you can recover a workflow instance if a task with a restart recovery strategy encounters a recoverable error, if you abort or cancel the workflow instance, or if the Data Integration Service process shuts down unexpectedly.

A workflow instance can abort for multiple reasons. View the workflow log to identify the cause of the interruption. After fixing any recoverable errors, you can recover the interrupted workflow instance if it is enabled for recovery.

You cannot change a workflow definition between the interrupted run and the recovery run. If a workflow instance has a recoverable state and you change the workflow metadata in the Developer tool and redeploy the application that contains the workflow, then the workflow instance is no longer recoverable.

When you recover a workflow instance, the Data Integration Service restarts or skips the interrupted task based on the task recovery strategy. The service continues processing the subsequent workflow objects. When a workflow instance runs in recovery mode, the contents panel on the Monitoring tab displays a blue arrow over the workflow and workflow object state icons. The contents panel lists each workflow instance and task once, even if you recover the workflow instance multiple times. When you expand a restarted Mapping task, the contents panel lists multiple mapping jobs if you recover the workflow instance multiple times.

A workflow instance can encounter the same states in a recovery run as in the original run. If the workflow instance encounters the state during a recovery run, the state has the text (Recovery) appended to it. For example, the state Completed (Recovery) means that the workflow instance was completed during a recovery run.

Recovery Properties

The read-only recovery properties display for each workflow instance. You configure the recovery properties for the workflow definition in the Developer tool. You cannot change the values of the properties for the workflow instance.

The following table describes the read-only recovery properties for a workflow instance:

Property	Description
Recovery Enabled	Indicates that the workflow is enabled for recovery.
Automatically Recovery Workflows	Indicates that the Data Integration Service process automatically recovers workflow instances that were aborted due to an unexpected service process shutdown. The workflow recovery starts after the Data Integration Service process restarts.
Maximum Recovery Attempts	Maximum number of times that a user or the Data Integration Service can attempt to recover the workflow instance.
Recovery Attempts	Number of recovery attempts made for this workflow instance. When a workflow instance reaches the maximum number of recovery attempts, the workflow instance is no longer recoverable.

Recovering a Workflow

You can recover aborted or canceled workflow instances that are enabled for recovery.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **Workflows**.
A list of workflow instances appear in the contents panel.
4. In the contents panel, select the aborted or canceled workflow instance that you want to recover.
5. Click **Actions > Recover Selected Workflow**.
Monitor the state of the workflow recovery run in the contents panel.

Workflow Logs

The Data Integration Service generates log events when you run a workflow instance. Log events include information about errors, task processing, expression evaluation in sequence flows, and workflow parameter and variable values.

If a workflow instance includes a Mapping task, the Data Integration Service generates a separate log file for the mapping. The mapping log file includes any errors encountered during the mapping run and load summary and transformation statistics.

You can view the workflow and mapping logs from the Monitoring tab.

When you recover an interrupted workflow instance, the Data Integration Service appends log events to the existing workflow log. When the recovered workflow instance includes a Mapping task that is restarted, the Data Integration Service appends log events to the existing mapping log.

If the workflow runs on a grid, the recovery of the workflow instance might run on a different node than the original workflow instance run. If the recovery runs on a different node and the log directory is not in a shared location, the Data Integration Service creates a log file with the same name on the current node.

Workflow Log File Format

The information in the workflow log file depends on the sequence of events during the workflow instance run. The amount of information that the Data Integration Service sends to the logs depends on the tracing level set for the workflow.

The Data Integration Service updates the log file with the following information when you run a workflow instance:

Workflow initialization messages

Contain information about the workflow name and instance ID, the parameter file used to run the workflow instance, and initial variable values.

Workflow processing messages

Contain information about expression evaluation results for conditional sequence flows, the tasks that ran, and the outgoing branch taken after using a gateway to make a decision.

Task processing messages

Contain information about input data passed to the task, the work item that the task completed, and output data passed from the task to the workflow. The information depends on the type of task.

The workflow log file displays the timestamp, thread name, severity level, message code, and message text for each log event.

Viewing Logs for a Workflow

You can download the log for a workflow instance to view the workflow instance details.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **Workflows**.
A list of workflow instances appear in the contents panel.
4. In the contents panel, select a workflow instance.
5. Click **Actions > View Logs for Selected Object**.
A dialog box appears with the option to open or save the log file.

Viewing Logs for a Mapping Run in a Workflow

You can download the log for a mapping run in a workflow to view the mapping details.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service.
3. In the Navigator, expand an application and select **Workflows**.
A list of workflow instances appear in the contents panel.
4. In the contents panel, expand a workflow instance.
5. Expand a Mapping task, and then select the mapping run by the task.
6. Click **Actions > View Logs for Selected Object**.
A dialog box appears with the option to open or save the log file.

Monitoring a Folder of Objects

You can view properties and statistics about all objects in a folder in the Navigator of the **Monitoring** tab. You can select one of the following folders: Jobs, Deployed Mapping Jobs, Logical Data Objects, SQL Data Services, Web Services, and Workflows.

You can apply a filter to limit the number of objects that appear in the contents panel. You can create custom filters based on a time range. Custom filters allow you to select particular dates and times for job start times, end times, and elapsed times. Custom filters also allow you to filter results based on multiple filter criteria.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, select the folder.
The contents panel shows a list of objects contained in the folder.
3. Right-click the header of the table to add or remove columns.
4. Select **Receive New Notifications** to dynamically display new jobs, operations, requests, or workflows in the **Monitoring** tab.
5. Enter filter criteria to reduce the number of objects that appear in the contents panel.
6. Select the object in the contents panel to view details about the object in the details panel.
The details panel shows more information about the object selected in the contents panel.
7. To view jobs that started around the same time as the selected job, click **Actions > View Context**.
The selected job and other jobs that started around the same time appear in the **Context View** tab. You can also view the context of connections, deployed mappings, requests, and workflows.
8. Click the **Close** button to close the **Context View** tab.

Viewing the Context of an Object

View the context of an object to view other objects of the same type that started around the same time as the selected object. You might view the context of an object to troubleshoot a problem or to get a high-level understanding of what is happening at a particular period of time. You can view the context of jobs, deployed mappings, connections, requests, and workflows.

For example, you notice that your deployed mapping failed. When you view the context of the deployed mapping, an unfiltered list of deployed mappings appears in a separate working view, showing you all deployed mappings that started around the same time as your deployed mapping. You notice that the other deployed mappings also failed. You determine that the cause of the problem is that the Data Integration Service was unavailable.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, expand a Data Integration Service and select the category of objects.
For example, select **Jobs**.
3. In the contents panel, select the object for which you want to view the context.
For example, select a job.
4. Click **Actions > View Context**.

Configuring the Date and Time Custom Filter

You can apply a custom filter on a Start Time or End Time column in the contents panel of the **Monitoring** tab to filter results.

1. Select Custom as the filter option for the Start Time or End Time column.
The **Custom Filter: Date and Time** dialog box appears.
2. Enter the date range using the specified date and time formats.
3. Click **OK**.

Configuring the Elapsed Time Custom Filter

You can apply a custom filter on an Elapsed Time column in the contents panel of the **Monitoring** tab to filter results.

1. Select Custom as the filter option for the Elapsed Time column.
The **Custom Filter: Elapsed Time** dialog box appears.
2. Enter the time range.
3. Click **OK**.

Configuring the Multi-Select Custom Filter

You can apply a custom filter on columns in the contents panel of the Monitoring tab to filter results based on multiple selections.

1. Select Custom as the filter option for the column.
The **Custom Filter: Multi-Select** dialog box appears.
2. Select one or more filters.
3. Click **OK**.

Monitoring an Object

You can monitor an object on the **Monitoring** tab. You can view information about the object, such as properties, run-time statistics, and run-time reports.

1. In the Administrator tool, click the **Monitoring** tab.
2. In the Navigator, select the object.
The contents panel shows multiple views that display different information about the object. The views that appear are based on the type of object selected in the Navigator.
3. Select a view to show information about the object.

CHAPTER 12

Domain Reports

This chapter includes the following topics:

- [Domain Reports Overview, 200](#)
- [License Management Report, 200](#)
- [Web Services Report, 207](#)

Domain Reports Overview

You can run the following domain reports from the Reports tab in the Administrator tool:

- **License Management Report.** Monitors the number of software options purchased for a license and the number of times a license exceeds usage limits. The License Management Report displays the license usage information such as CPU and repository usage and the node configuration details.
- **Web Services Report.** Monitors activities of the web services running on a Web Services Hub. The Web Services Report displays run-time information such as the number of successful or failed requests and average service time. You can also view historical statistics for a specific period of time.

Note: If the master gateway node runs on a UNIX machine and the UNIX machine does not have a graphics display server, you must install X Virtual Frame Buffer on the UNIX machine to view the report charts in the License Report or the Web Services Report. If you have multiple gateway nodes running on UNIX machines, install X Virtual Frame Buffer on each UNIX machine.

License Management Report

You can monitor the list of software options purchased with a license and the number of times a license exceeds usage limits. The License Management Report displays the general properties, CPU and repository usage, user details, hardware and node configuration details, and the options purchased for each license.

You can save the License Management Report as a PDF on your local machine. You can also email a PDF version of the report to someone.

Run the License Management Report to monitor the following license usage information:

- **Licensing details.** Shows general properties for every license assigned in the domain.
- **CPU usage.** Shows the number of logical CPUs used to run application services in the domain. The License Management Report counts logical CPUs instead of physical CPUs for license enforcement. If the

number of logical CPUs exceeds the number of authorized CPUs, then the License Management Report shows that the domain exceeded the CPU limit.

- Repository usage. Shows the number of PowerCenter Repository Services in the domain.
- User information. Shows information about users in the domain.
- Hardware configuration. Shows details about the machines used in the domain.
Node configuration. Shows details about each node in the domain.
- Licensed options. Shows a list of PowerCenter and other Informatica options purchased for each license.

Licensing

The Licensing section of the License Management Report shows information about each license in the domain.

The following table describes the licensing information in the License Management Report:

Property	Description
Name	Name of the license.
Edition	PowerCenter edition.
Version	Version of Informatica platform.
Expiration Date	Date when the license expires.
Serial Number	Serial number of the license. The serial number identifies the customer or project. If the customer has multiple PowerCenter installations, there is a separate serial number for each project. The original and incremental keys for a license have the same serial number.
Deployment Level	Level of deployment. Values are Development and Production.
Operating System / BitMode	Operating system and bitmode for the license. Indicates whether the license is installed on a 32-bit or 64-bit operating system.
CPU	Maximum number of authorized logical CPUs.
Repository	Maximum number of authorized PowerCenter repositories.
AT Named Users	Maximum number of users who are assigned the License Access for Informatica Analyst privilege.
Product Bitmode	Bitmode of the server binaries that are installed. Values are 32-bit or 64-bit.

CPU Summary

The CPU Summary section of the License Management Report shows the maximum number of logical CPUs used to run application services in the domain. Use the CPU summary information to determine if the CPU usage exceeded the license limits. If the number of logical CPUs is greater than the total number of CPUs authorized by the license, the License Management Report indicates that the CPU limit is exceeded.

The License Management Report determines the number of logical CPUs based on the number of processors, cores, and threads. Use the following formula to calculate the number of logical CPUs:

$N * C * T$, where

N is the number of processors.

C is the number of cores in each processor.

T is the number of threads in each core.

For example, a machine contains 4 processors. Each processor has 2 cores. The machine contains 8 (4*2) physical cores. Hyperthreading is enabled, where each core contains 3 threads. The number of logical CPUs is 24 (4*2*3).

Note: Although the License Management Report includes threads in the calculation of logical CPUs, Informatica license compliance is based on the number of physical cores, not threads. To be compliant, the number of physical cores must be less than or equal to the maximum number of licensed CPUs. If the License Management Report shows that you have exceeded the license limit but the number of physical cores is less than or equal to the maximum number of licensed CPUs, you can ignore the message. If you have a concern about license compliance, contact your Informatica account manager.

The following table describes the CPU summary information in the License Management Report:

Property	Description
Domain	Name of the domain on which the report runs.
Current Usage	Maximum number of logical CPUs used concurrently on the day the report runs.
Peak Usage	Maximum number of logical CPUs used concurrently during the last 12 months.
Peak Usage Date	Date when the maximum number of logical CPUs were used concurrently during the last 12 months.
Days Exceeded License Limit	Number of days that the CPU usage exceeded the license limits. The domain exceeds the CPU license limit when the number of concurrent logical CPUs exceeds the number of authorized CPUs.

CPU Detail

The CPU Detail section of the License Management Report provides CPU usage information for each host in the domain. The CPU Detail section shows the maximum number of logical CPUs used each day in a selected time period.

The report counts the number of logical CPUs on each host that runs application services in the domain. The report groups logical CPU totals by node.

The following table describes the CPU detail information in the License Management Report:

Property	Description
Host Name	Host name of the machine.
Current Usage	Maximum number of logical CPUs that the host used concurrently on the day the report runs.
Peak Usage	Maximum number of logical CPUs that the host used concurrently during the last 12 months.

Property	Description
Peak Usage Date	Date in the last 12 months when the host concurrently used the maximum number of logical CPUs.
Assigned Licenses	Name of all licenses assigned to services that run on the node.

Repository Summary

The Repository Summary section of the License Management Report provides repository usage information for the domain. Use the repository summary information to determine if the repository usage exceeded the license limits.

The following table describes the repository summary information in the License Management Report:

Property	Description
Current Usage	Maximum number of repositories used concurrently in the domain on the day the report runs.
Peak Usage	Maximum number of repositories used concurrently in the domain during the last 12 months.
Peak Usage Date	Date in the last 12 months when the maximum number of repositories were used concurrently.
Days Exceeded License Limit	Number of days that the repository usage exceeded the license limits.

User Summary

The User Summary section of the License Management Report provides information about Analyst tool users in the domain.

The following table describes the user summary information in the License Management Report:

Property	Description
User Type	Type of user in the domain.
Current Named Users	Maximum number of users who are assigned the License Access for Informatica Analyst privilege on the day the report runs.
Peaked Name Users	Maximum number of users who are assigned the License Access for Informatica Analyst privilege during the last 12 months.
Peak Named Users Date	Date during the last 12 months when the maximum number of concurrent users were assigned the License Access for Informatica Analyst privilege.

User Detail

The User Detail section of the License Management Report provides information about each Analyst tool user in the domain.

The following table describes the user detail information in the License Management Report:

Property	Description
User Type	Type of user in the domain.
User Name	User name.
Days Logged In	Number of days the user logged in to the Analyst tool and performed profiling during the last 12 months.
Peak Unique IP Addresses in a Day	Maximum number of machines that the user was logged in to and performed profiling on during a single day of the last 12 months.
Average Unique IP Addresses	Daily average number of machines that the user was logged in to and running profiling on during the last 12 months.
Peak IP Address Date	Date when the user logged in to and performed profiling on the maximum number of machines during a single day of the last 12 months.
Peak Daily Sessions	Maximum number of times in a single day of the last 12 months that the user logged in to any Analyst tool and performed profiling.
Average Daily Sessions	Average number of times per day in the last 12 months that the user logged in to any Analyst tool and performed profiling.
Peak Session Date	Date in the last 12 months when the user had the most daily sessions in the Analyst tool.

Hardware Configuration

The Hardware Configuration section of the License Management Report provides details about machines used in the domain.

The following table describes the hardware configuration information in the License Management Report:

Property	Description
Host Name	Host name of the machine.
Logical CPUs	Number of logical CPUs used to run application services in the domain.
Cores	Number of cores used to run application services in the domain.
Sockets	Number of sockets on the machine.
CPU Model	Model of the CPU.
Hyperthreading Enabled	Indicates whether hyperthreading is enabled.
Virtual Machine	Indicates whether the machine is a virtual machine.

Node Configuration

The Node Configuration section of the License Management Report provides details about each node in the domain.

The following table describes the node configuration information in the License Management Report:

Property	Description
Node Name	Name of the node or nodes assigned to a machine for a license.
Host Name	Host name of the machine.
IP Address	IP address of the node.
Operating System	Operating system of the machine on which the node runs.
Status	Status of the node.
Gateway	Indicates whether the node is a gateway node.
Service Type	Type of the application service configured to run on the node.
Service Name	Name of the application service configured to run on the node.
Service Status	Status of the application service.
Assigned License	License assigned to the application service.

Licensed Options

The Licensed Options section of the License Management Report provides details about each option for every license assigned to the domain.

The following table describes the licensed option information in the License Management Report:

Property	Description
License Name	Name of the license.
Description	Name of the license option.
Status	Status of the license option.
Issued On	Date when the license option was issued.
Expires On	Date when the license option expires.

Running the License Management Report

Run the License Management Report from the **Reports** tab in the Administrator tool.

1. Click the **Reports** tab in the Administrator tool.
2. Click the **License Management Report** view.

The License Management Report appears.

3. Click **Save** to save the License Management Report as a PDF.

If a License Management Report contains multibyte characters, you must configure the Service Manager to use a Unicode font.

4. Click **Email** to send a copy of the License Management Report in an email.

The **Send License Management Report** page appears.

Configuring a Unicode Font for the Report

Before you can save a License Management Report that contains multibyte characters or non-English characters, configure the Service Manager to use a Unicode font when generating the PDF file.

1. Install a Unicode font on the master gateway node.
2. Use a text editor to create a file named `AcUtil.properties`.
3. Add the following properties to the file:

```
PDF.Font.Default=Unicode_font_name
PDF.Font.MultibyteList=Unicode_font_name
```

Unicode_font_name is the name of the Unicode font installed on the master gateway node.

You might also need to add the following property if the font file is not available in the locale:

```
Unicode_font_name_path=Unicode_font_file_location
```

For example:

```
PDF.Font.Default=Arial Unicode MS
PDF.Font.MultibyteList=Arial Unicode MS
Arial Unicode MS_path=/usr/lib/X11/fonts/TrueType
```

4. Save the `AcUtil.properties` file to the following location:

```
InformaticaInstallationDir\services\AdministratorConsole\administrator
```

5. Use a text editor to open the `licenseUtility.css` file in the following location:

```
InformaticaInstallationDir\services\AdministratorConsole\administrator\css
```

6. Append the Unicode font name to the value of each font-family property.

For example:

```
font-family: Arial Unicode MS, Verdana, Arial, Helvetica, sans-serif;
```

7. Restart Informatica services on each node in the domain.

Sending the License Management Report in an Email

You must configure the SMTP settings for the domain before you can send the License Management Report in an email.

The domain administrator can send the License Management Report in an email from Send License Management Report page in the Administrator tool.

1. Enter the following information:

Property	Description
To Email	Email address to which you send the License Management Report.
Subject	Subject of the email.
Customer Name	Name of the organization that purchased the license.
Request ID	Request ID that identifies the project for which the license was purchased.
Contact Name	Name of the contact person in the organization.
Contact Phone Number	Phone number of the contact person.
Contact Email	Email address of the contact person at the customer site.

2. Click OK.

The Administrator tool sends the License Management Report in an email.

Web Services Report

To analyze the performance of web services running on a Web Services Hub, you can run a report for the Web Services Hub or for a web service running on the Web Services Hub.

The Web Services Report provides run-time and historical information on the web service requests handled by the Web Services Hub. The report displays aggregated information for all web services in the Web Services Hub and information for each web service running on the Web Services Hub. The Web Services Report also provides historical information.

Understanding the Web Services Report

You can run the Web Services Report for a time interval that you choose. The Web Services Hub collects information on web services activities and caches 24 hours of information for use in the Web Services Report. It also writes the information to a history file.

Time Interval

By default, the Web Services Report displays activity information for a five-minute interval. You can select one of the following time intervals to display activity information for a web service or Web Services Hub:

- 5 seconds
- 1 minute
- 5 minutes
- 1 hour
- 24 hours

The Web Services Report displays activity information for the interval ending at the time you run the report. For example, if you run the Web Services Report at 8:05 a.m. for an interval of one hour, the Web Services Report displays the Web Services Hub activity from 7:05 a.m. and 8:05 a.m.

Caching

The Web Services Hub caches 24 hours of activity data. The cache is reinitialized every time the Web Services Hub is restarted. The Web Services Report displays statistics from the cache for the time interval that you run the report.

History File

The Web Services Hub writes the cached activity data to a history file. The Web Services Hub stores data in the history file for the number of days that you set in the MaxStatsHistory property of the Web Services Hub. For example, if the value of the MaxStatsHistory property is 5, the Web Services Hub keeps five days of data in the history file.

Contents of the Web Services Report

The Web Services Report displays information in different views and panels of the Informatica tool. The Web Services Hub report includes the following information:

- **General Properties and Web Services Hub Summary.** To view the general properties and summary information for the Web Services Hub, select the Properties view in the content panel. The Properties view displays the information.
- **Web Services Historical Statistics.** To view historical statistics for the web services in the Web Services Hub, select the Properties view in the content panel. The detail panel displays a table of historical statistics for the date that you specify.
- **Web Services Run-Time Statistics.** To view run-time statistics for each web service in the Web Services Hub, select the Web Services view in the content panel. The Web Services view lists the statistics for each web service.
- **Web Service Properties.** To view the properties of a web service, select the web service in the Web Services view of the content panel. In the details panel, the Properties view displays the properties for the web service.
- **Web Service Top IP Addresses.** To view the top IP addresses for a web service, select a web service in the Web Services view of the content panel and select the Top IP Addresses view in the details panel. The detail panel displays the most active IP addresses for the web service.
- **Web Service Historical Statistics.** To view a table of historical statistics for a web service, select a web service in the Web Services view of the content panel and select the Table view in the details panel. The detail panel displays a table of historical statistics for the web service.

General Properties and Web Services Hub Summary

To view the general properties and summary information for the Web Services Hub, select the Properties view in the content panel.

The following table describes the general properties:

Property	Description
Name	Name of the Web Services Hub.
Description	Short description of the Web Services Hub.
Service type	Type of Service. For a Web Services Hub, the service type is ServiceWSHubService.

The following table describes the Web Services Hub Summary properties:

Property	Description
# of Successful Message	Number of requests that the Web Services Hub processed successfully.
# of Fault Responses	Number of fault responses generated by web services in the Web Services Hub. The fault responses could be due to any error.
Total Messages	Total number of requests that the Web Services Hub received.
Last Server Restart Tme	Date and time when the Web Services Hub was last started.
Avg. # of Service Partitions	Average number of partitions allocated for all web services in the Web Services Hub.
% of Partitions in Use	Percentage of web service partitions that are in use for all web services in the Web Services Hub.
Avg. # of Run Instances	Average number of instances running for all web services in the Web Services Hub.

Web Services Historical Statistics

To view historical statistics for the web services in the Web Services Hub, select the Properties view in the content panel. The detail panel displays data from the Web Services Hub history file for the date that you specify.

The following table describes the historical statistics:

Property	Description
Time	Time of the event.
Web Service	Name of the web service for which the information is displayed. When you click the name of a web service, the Web Services Report displays the Service Statistics window.

Property	Description
Successful Requests	Number of requests successfully processed by the web service.
Fault Responses	Number of fault responses sent by the web service.
Avg. Service Time	Average time it takes to process a service request received by the web service.
Max Service Time	The largest amount of time taken by the web service to process a request.
Min Service Time	The smallest amount of time taken by the web service to process a request.
Avg. DTM Time	Average number of seconds it takes the PowerCenter Integration Service to process the requests from the Web Services Hub.
Avg. Service Partitions	Average number of session partitions allocated for the web service.
Percent Partitions in Use	Percentage of partitions in use by the web service.
Avg Run Instances	Average number of instances running for the web service.

Web Services Run-time Statistics

To view run-time statistics for each web service in the Web Services Hub, select the Web Services view in the content panel. The Web Services view lists the statistics for each web service.

The report provides the following information for each web service for the selected time interval:

Property	Description
Service name	Name of the web service for which the information is displayed.
Successful Requests	Number of requests received by the web service that the Web Services Hub processed successfully.
Fault Responses	Number of fault responses generated by the web services in the Web Services Hub.
Avg. Service Time	Average time it takes to process a service request received by the web service.
Avg. Service Partitions	Average number of session partitions allocated for the web service.
Avg. Run Instances	Average number of instances of the web service running during the interval.

Web Service Properties

To view the properties of a web service, select the web service in the Web Services view of the content panel. In the details panel, the Properties view displays the properties for the web service.

The report provides the following information for the selected web service:

Property	Description
# of Successful Requests	Number of requests received by the web service that the Web Services Hub processed successfully.
# of Fault Responses	Number of fault responses generated by the web services in the Web Services Hub.
Total Messages	Total number of requests that the Web Services Hub received.
Last Server Restart Time	Date and time when the Web Services Hub was last started
Last Service Time	Number of seconds it took to process the most recent service request
Average Service Time	Average time it takes to process a service request received by the web service.
Avg.# of Service Partitions	Average number of session partitions allocated for the web service.
Avg. # of Run Instances	Average number of instances of the web service running during the interval.

Web Service Top IP Addresses

To view the top IP addresses for a web service, select a web service in the Web Services view of the content panel and select the Top IP Addresses view in the details panel. The Top IP Addresses displays the most active IP addresses for the web service, listed in the order of longest to shortest service times.

The report provides the following information for each of the most active IP addresses:

Property	Description
Top 10 Client IP Addresses	The list of client IP addresses and the longest time taken by the web service to process a request from the client. The client IP addresses are listed in the order of longest to shortest service times. Use the Click here link to display the list of IP addresses and service times.

Web Service Historical Statistics Table

To view a table of historical statistics for a web service, select a web service in the Web Services view of the content panel and select the Table view in the details panel. The details panel displays a table of historical statistics for the web service.

The table provides the following information for the selected web service:

Property	Description
Time	Time of the event.
Web Service	Name of the web service for which the information is displayed.
Successful Requests	Number of requests successfully processed by the web service.
Fault Responses	Number of requests received for the web service that could not be processed and generated fault responses.
Avg. Service Time	Average time it takes to process a service request received by the web service.
Min. Service Time	The smallest amount of time taken by the web service to process a request.
Max. Service Time	The largest amount of time taken by the web service to process a request.
Avg. DTM Time	Average time it takes the PowerCenter Integration Service to process the requests from the Web Services Hub.
Avg. Service Partitions	Average number of session partitions allocated for the web service.
Percent Partitions in Use	Percentage of partitions in use by the web service.
Avg. Run Instances	Average number of instances running for the web service.

Running the Web Services Report

Run the Web Services Report from the Reports tab in the Administrator tool.

Before you run the Web Services Report for a Web Services Hub, verify that the Web Services Hub is enabled. You cannot run the Web Services Report for a disabled Web Services Hub.

1. In the Administrator tool, click the Reports tab.
2. Click Web Services.
3. In the Navigator, select the Web Services Hub for which to run the report.
In the content panel, the Properties view displays the properties of the Web Services Hub. The details view displays historical statistics for the services in the Web Services Hub.
4. To specify a date for historical statistics, click the date filter icon in the details panel, and select the date.
5. To view information about each service, select the Web Services view in the content panel.
The Web Services view displays summary statistics for each service for the Web Services Hub.
6. To view additional information about a service, select the service from the list.
In the details panel, the Properties view displays the properties for the service.
7. To view top IP addresses for the service, select the Top IP Addresses view in the details panel.
8. To view table attributes for the service, select the Table view in the detail panel.

Running the Web Services Report for a Secure Web Services Hub

To run a Web Services Hub on HTTPS, you must have an SSL certificate file for authentication of message transfers. When you create a Web Services Hub to run on HTTPS, you must specify the location of the

keystore file that contains the certificate for the Web Services Hub. To run the Web Services Report in the Administrator tool for a secure Web Services Hub, you must import the SSL certificate into the Java certificate file. The Java certificate file is named *cacerts* and is located in the */lib/security* directory of the Java directory. The Administrator tool uses the *cacerts* certificate file to determine whether to trust an SSL certificate.

In a domain that contains multiple nodes, the node where you generate the SSL certificate affects how you access the Web Services Report for a secure Web Services Hub.

Use the following rules and guidelines to run the Web Services Report for a secure Web Services Hub in a domain with multiple nodes:

- For each secure Web Services Hub running in a domain, generate an SSL certificate and import it to a Java certificate file.
- The Administrator tool searches for SSL certificates in the certificate file of a gateway node. The SSL certificate for a Web Services Hub running on worker node must be generated on a gateway node and imported into the certificate file of the same gateway node.
- To view the Web Services Report for a secure Web Services Hub, log in to the Administrator tool from the gateway node that has the certificate file containing the SSL certificate of the Web Services Hub for which you want to view reports.
- If a secure Web Services Hub runs on a worker node, the SSL certificate must be generated and imported into the certificate file of the gateway node. If a secure Web Services Hub runs on a gateway and a worker node, the SSL certificate of both nodes must be generated and imported into the certificate file of the gateway node. To view reports for the secure Web Services Hub, log in to the Administrator tool from the gateway node.
- If the domain has two gateway nodes and a secure Web Services Hub runs on each gateway node, access to the Web Services Reports depends on where the SSL certificate is located.

For example, gateway node GWN01 runs Web Services Hub WSH01 and gateway node GWN02 runs Web Services Hub WSH02. You can view the reports for the Web Services Hubs based on the location of the SSL certificates:

- If the SSL certificate for WSH01 is in the certificate file of GWN01 but not GWN02, you can view the reports for WSH01 if you log in to the Administrator tool through GWN01. You cannot view the reports for WSH01 if you log in to the Administrator tool through GWN02. If GWN01 fails, you cannot view reports for WSH01.
- If the SSL certificate for WSH01 is in the certificate files of GWN01 and GWN02, you can view the reports for WSH01 if you log in to the Administrator tool through GWN01 or GWN02. If GWN01 fails, you can view the reports for WSH01 if you log in to the Administrator tool through GWN02.
- To ensure successful failover when a gateway node fails, generate and import the SSL certificates of all Web Services Hubs in the domain into the certificates files of all gateway nodes in the domain.

CHAPTER 13

Node Diagnostics

This chapter includes the following topics:

- [Node Diagnostics Overview, 214](#)
- [Informatica MySupport Portal Login, 215](#)
- [Generating Node Diagnostics, 216](#)
- [Downloading Node Diagnostics, 216](#)
- [Uploading Node Diagnostics, 217](#)
- [Analyzing Node Diagnostics, 218](#)

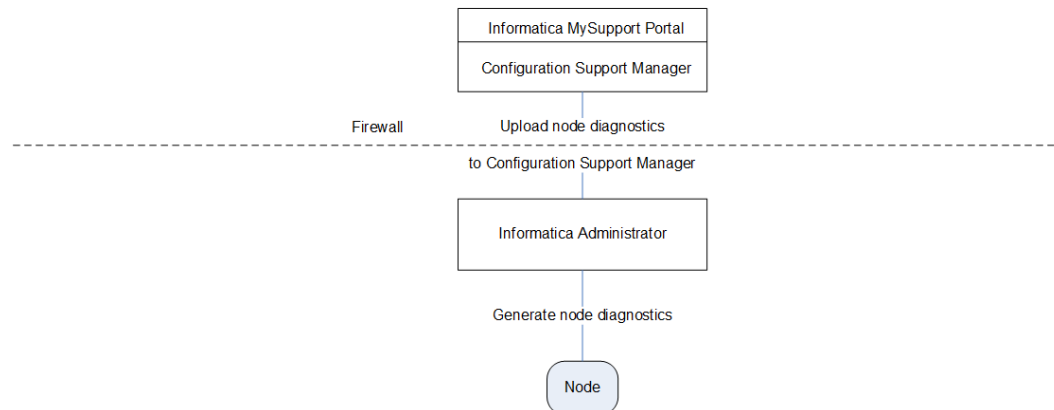
Node Diagnostics Overview

The Configuration Support Manager is a web-based application that you can use to track Informatica updates and diagnose issues in your environment.

You can discover comprehensive information about your technical environment and diagnose issues before they become critical.

Generate node diagnostics from the Informatica Administrator and upload them to the Configuration Support Manager in the Informatica MySupport Portal. Then, check the node diagnostics against business rules and recommendations in the Configuration Support Manager.

The following image shows the operational flow to generate and upload node diagnostics:



Complete the following tasks to generate and upload node diagnostics:

1. Log in to the Informatica MySupport Portal.

2. Generate node diagnostics. The Service Manager analyzes the services of the node and generates node diagnostics including information such as operating system details, CPU details, database details, and patches.
3. Optionally, download node diagnostics to your local drive.
4. Upload node diagnostics to the Configuration Support Manager, a diagnostic web application outside the firewall. The Configuration Support Manager is a part of the Informatica MySupport Portal. The Service Manager connects to the Configuration Support Manager through the HTTPS protocol and uploads the node diagnostics.
5. Review the node diagnostics in the Configuration Support Manager to find troubleshooting information for your environment.

Informatica MySupport Portal Login

You must log in to the customer portal to upload node diagnostics to the Configuration Support Manager. The login credentials are not specific to a user. The same credentials are applicable for all users who have access to the Administrator tool. Register at <http://communities.informatica.com> if you do not have the customer portal login details. You need to enter the customer portal login details and, then save these details. Alternatively, you can enter the customer portal details each time you upload node diagnostics to the Configuration Support Manager. You can generate node diagnostics without entering the login details.

To maintain login security, you must log out of the Configuration Support Manager and the Node Diagnostics Upload page of the Administrator tool.

- To log out of the Configuration Support Manager, click the logout link.
- To log out of the Upload page, click **Close Window**.

Note: If you close these windows through the web browser close button, you remain logged in to the Configuration Support Manager. Other users can access the Configuration Support Manager without valid credentials.

Logging In to the Informatica MySupport Portal

Before you generate and upload node diagnostics, you must log in to the Informatica My Support Portal.

1. In the Administrator tool, click **Domain**.
2. In the Navigator, select the domain.
3. In the contents panel, click **Diagnostics**.
A list of all the nodes in the domain appears.
4. Click **Edit Customer Portal Login Credentials**.

The **Edit Customer Portal Login Credentials** dialog box appears.

Note: You can also edit portal credentials from the **Actions** menu on the **Diagnostics** tab.

5. Enter the following customer portal login details:

Field	Description
Email Address	Email address with which you registered your customer portal account.
Password	Password for your customer portal account.
Project ID	Unique ID assigned to your support project.

6. Click **OK**.

Generating Node Diagnostics

When you generate node diagnostics, the Administrator tool generates node diagnostics in an XML file.

The XML file contains details about services, logs, environment variables, operating system parameters, system information, and database clients. Node diagnostics of worker nodes do not include domain metadata information but contain only node metadata information.

1. In the Administrator tool, click **Domain**.
2. In the Navigator, select the domain.
3. In the contents panel, click **Diagnostics**.
A list of all nodes in the domain appears.
4. Select the node.
5. Click **Generate Diagnostics File**.
6. Click **Yes** to confirm that you want to generate node diagnostics.

Note: You can also generate diagnostics from the **Actions** menu on the **Diagnostics** tab.

The `csmagent<host name>.xml` file, which contains the node diagnostics, is generated at `INFA_HOME/server/csm/output`. The node diagnostics and the time stamp of the generated file appear.

7. To run diagnostics for your environment, upload the `csmagent<host name>.xml` file to the Configuration Support Manager.

Alternatively, you can download the XML file to your local drive.

After you generate node diagnostics for the first time, you can regenerate or upload them.

Downloading Node Diagnostics

After you generate node diagnostics, you can download it to your local drive.

1. In the Administrator tool, click **Domain**.
2. In the Navigator, select the domain.
3. In the contents panel, click **Diagnostics**.

A list of all nodes in the domain appears.

4. Click the diagnostics file name of the node.

The file opens in another browser window.

5. Click **File > Save As**. Then, specify a location to save the file.

6. Click **Save**.

The XML file is saved to your local drive.

Uploading Node Diagnostics

You can upload node diagnostics to the Configuration Support Manager through the Administrator tool. You must enter the customer portal login details before you upload node diagnostics.

When you upload node diagnostics, you can update or create a configuration in the Configuration Support Manager. Create a configuration the first time you upload the node diagnostics. Update a configuration to view the latest diagnostics of the configuration. To compare current and previous node configurations of an existing configuration, upload the current node diagnostics as a new configuration.

Note: If you do not have access to the Internet, you can download the file and upload it at a later time. You can also send the file to the Informatica Global Customer Support in an email to troubleshoot or to upload.

1. In the Administrator tool, click **Domain**.
2. In the Navigator, select the domain.
3. In the contents panel, click **Diagnostics**.

A list of all nodes in the domain appears.

4. Select the node.
5. Generate node diagnostics.
6. Click **Upload Diagnostics File to CSM**.

You can upload the node diagnostics as a new configuration or as an update to an existing configuration.

7. To upload a new configuration, go to step [10](#).
- To update a configuration, select **Update an existing configuration**.
8. Select the configuration you want to update from the list of configurations.
9. Go to step [12](#).
10. Select **Upload as a new configuration**.
11. Enter the following configuration details:

Field	Description
Name	Configuration name.
Description	Configuration description.
Type	Type of the node, which is one of the following types: <ul style="list-style-type: none">- Production- Development- Test/QA

12. Click **Upload Now**.

After you upload the node diagnostics, go to the Configuration Support Manager to analyze the node diagnostics.

13. Click **Close Window**.

Note: If you close the window by using the close button in the browser, the user authentication session does not end and you cannot upload node diagnostics to the Configuration Support Manager with another set of customer portal login credentials.

Analyzing Node Diagnostics

Use the Configuration Support Manager to analyze node diagnostics.

Use the Configuration Support Manager to complete the following tasks:

- Diagnose issues before they become critical.
- Identify bug fixes.
- Identify recommendations that can reduce risk of unplanned outage.
- View details of your technical environment.
- Manage your configurations efficiently.
- Subscribe to proactive alerts through email and RSS.
- Run advanced diagnostics with compare configuration.

Identify Bug Fixes

You can use the Configuration Support Manager to resolve issues encountered during operations. To expedite resolution of support issues, you can generate and upload node diagnostics to the Configuration Support Manager. You can analyze node diagnostics in the Configuration Support Manager and find a solution to your issue.

For example, when you run a Sorter session that processes a large volume of data, you notice that there is some data loss. You generate node diagnostics and upload them to the Configuration Support Manager. When you review the diagnostics for bug fix alerts, you see that a bug fix, EBF178626, is available for this. You apply EBF178626, and run the session again. All data is successfully loaded.

Identify Recommendations

You can use the Configuration Support Manager to avoid issues in your environment. You can troubleshoot issues that arise after you make changes to the node properties by comparing different node diagnostics in the Configuration Support Manager. You can also use the Configuration Support Manager to identify recommendations or updates that may help you improve the performance of the node.

For example, you upgrade the node memory to handle a higher volume of data. You generate node diagnostics and upload them to the Configuration Support Manager. When you review the diagnostics for operating system warnings, you find the recommendation to increase the total swap memory of the node to twice that of the node memory for optimal performance. You increase swap space as suggested in the Configuration Support Manager and avoid performance degradation.

Tip: Regularly upload node diagnostics to the Configuration Support Manager and review node diagnostics to maintain your environment efficiently.

CHAPTER 14

Understanding Globalization

This chapter includes the following topics:

- [Globalization Overview, 219](#)
- [Locales, 221](#)
- [Data Movement Modes, 222](#)
- [Code Page Overview, 224](#)
- [Code Page Compatibility, 226](#)
- [Code Page Validation, 233](#)
- [Relaxed Code Page Validation, 234](#)
- [PowerCenter Code Page Conversion, 236](#)
- [Case Study: Processing ISO 8859-1 Data, 237](#)
- [Case Study: Processing Unicode UTF-8 Data, 239](#)

Globalization Overview

Informatica can process data in different languages. Some languages require single-byte data, while other languages require multibyte data. To process data correctly in Informatica, you must set up the following items:

- **Locale.** Informatica requires that the locale settings on machines that access Informatica applications are compatible with code pages in the domain. You may need to change the locale settings. The locale specifies the language, territory, encoding of character set, and collation order.
- **Data movement mode.** The PowerCenter Integration Service can process single-byte or multibyte data and write it to targets. Use the ASCII data movement mode to process single-byte data. Use the Unicode data movement mode for multibyte data.
- **Code pages.** Code pages contain the encoding to specify characters in a set of one or more languages. You select a code page based on the type of character data you want to process. To ensure accurate data movement, you must ensure compatibility among code pages for Informatica and environment components. You use code pages to distinguish between US-ASCII (7-bit ASCII), ISO 8859-1 (8-bit ASCII), and multibyte characters.

To ensure data passes accurately through your environment, the following components must work together:

- Domain configuration database code page
- Administrator tool locale settings and code page
- PowerCenter Integration Service data movement mode

- Code page for each PowerCenter Integration Service process
- PowerCenter Client code page
- PowerCenter repository code page
- Source and target database code pages
- Metadata Manager repository code page

You can configure the PowerCenter Integration Service for relaxed code page validation. Relaxed validation removes restrictions on source and target code pages.

Unicode

The Unicode Standard is the work of the Unicode Consortium, an international body that promotes the interchange of data in all languages. The Unicode Standard is designed to support any language, no matter how many bytes each character in that language may require. Currently, it supports all common languages and provides limited support for other less common languages. The Unicode Consortium is continually enhancing the Unicode Standard with new character encodings. For more information about the Unicode Standard, see <http://www.unicode.org>.

The Unicode Standard includes multiple character sets. Informatica uses the following Unicode standards:

- UCS-2 (Universal Character Set, double-byte). A character set in which each character uses two bytes.
- UTF-8 (Unicode Transformation Format). An encoding format in which each character can use between one to four bytes.
- UTF-16 (Unicode Transformation Format). An encoding format in which each character uses two or four bytes.
- UTF-32 (Unicode Transformation Format). An encoding format in which each character uses four bytes.
- GB18030. A Unicode encoding format defined by the Chinese government in which each character can use between one to four bytes.

Informatica is a Unicode application. The PowerCenter Client, PowerCenter Integration Service, and Data Integration Service use UCS-2 internally. The PowerCenter Client converts user input from any language to UCS-2 and converts it from UCS-2 before writing to the PowerCenter repository. The PowerCenter Integration Service and Data Integration Service converts source data to UCS-2 before processing and converts it from UCS-2 after processing. The PowerCenter repository, Model repository, PowerCenter Integration Service, and Data Integration Service support UTF-8. You can use Informatica to process data in any language.

Working with a Unicode PowerCenter Repository

The PowerCenter repository code page is the code page of the data in the PowerCenter repository. You choose the PowerCenter repository code page when you create or upgrade a PowerCenter repository. When the PowerCenter repository database code page is UTF-8, you can create a PowerCenter repository using the UTF-8 code page.

The domain configuration database uses the UTF-8 code page. If you need to store metadata in multiple languages, such as Chinese, Japanese, and Arabic, you must use the UTF-8 code page for all services in that domain.

The Service Manager synchronizes the list of users in the domain with the list of users and groups in each application service. If a user in the domain has characters that the code page of the application services does not recognize, characters do not convert correctly and inconsistencies occur.

Use the following guidelines when you use UTF-8 as the PowerCenter repository code page:

- The PowerCenter repository database code page must be UTF-8.
- The PowerCenter repository code page must be a superset of the PowerCenter Client and PowerCenter Integration Service process code pages.
- You can input any character in the UCS-2 character set. For example, you can store German, Chinese, and English metadata in a UTF-8 enabled PowerCenter repository.
- Install languages and fonts on the PowerCenter Client machine. If you are using a UTF-8 PowerCenter repository, you may want to enable the PowerCenter Client machines to display multiple languages. By default, the PowerCenter Clients display text in the language set in the system locale. Use the Regional Options tool in the Control Panel to add language groups to the PowerCenter Client machines.
- You can use the Windows Input Method Editor (IME) to enter multibyte characters from any language without having to run the version of Windows specific for that language.
- Choose a code page for a PowerCenter Integration Service process that can process all PowerCenter repository metadata correctly. The code page of the PowerCenter Integration Service process must be a subset of the PowerCenter repository code page. If the PowerCenter Integration Service has multiple service processes, ensure that the code pages for all PowerCenter Integration Service processes are subsets of the PowerCenter repository code page. If you are running the PowerCenter Integration Service process on Windows, the code page for the PowerCenter Integration Service process must be the same as the code page for the system or user locale. If you are running the PowerCenter Integration Service process on UNIX, use the UTF-8 code page for the PowerCenter Integration Service process.

Locales

Every machine has a locale. A locale is a set of preferences related to the user environment, including the input language, keyboard layout, how data is sorted, and the format for currency and dates. Informatica uses locale settings on each machine.

You can set the following locale settings on Windows:

- System locale. Determines the language, code pages, and associated bitmap font files that are used as defaults for the system.
- User locale. Determines the default formats to display date, time, currency, and number formats.
- Input locale. Describes the input method, such as the keyboard, of the system language.

For more information about configuring the locale settings on Windows, consult the Windows documentation.

System Locale

The system locale is also referred to as the system default locale. It determines which ANSI and OEM code pages, as well as bitmap font files, are used as defaults for the system. The system locale contains the language setting, which determines the language in which text appears in the user interface, including in dialog boxes and error messages. A message catalog file defines the language in which messages display. By default, the machine uses the language specified for the system locale for all processes, unless you override the language for a specific process.

The system locale is already set on your system and you may not need to change settings to run Informatica. If you do need to configure the system locale, you configure the locale on a Windows machine in the Regional Options dialog box. On UNIX, you specify the locale in the LANG environment variable.

User Locale

The user locale displays date, time, currency, and number formats for each user. You can specify different user locales on a single machine. Create a user locale if you are working with data on a machine that is in a different language than the operating system. For example, you might be an English user working in Hong Kong on a Chinese operating system. You can set English as the user locale to use English standards in your work in Hong Kong. When you create a new user account, the machine uses a default user locale. You can change this default setting once the account is created.

Input Locale

An input locale specifies the keyboard layout of a particular language. You can set an input locale on a Windows machine to type characters of a specific language.

You can use the Windows Input Method Editor (IME) to enter multibyte characters from any language without having to run the version of Windows specific for that language. For example, if you are working on an English operating system and need to enter text in Chinese, you can use IME to set the input locale to Chinese without having to install the Chinese version of Windows. You might want to use an input method editor to enter multibyte characters into a PowerCenter repository that uses UTF-8.

Data Movement Modes

The data movement mode is a PowerCenter Integration Service option you choose based on the type of data you want to move, single-byte or multibyte data. The data movement mode you select depends the following factors:

- Requirements to store single-byte or multibyte metadata in the PowerCenter repository
- Requirements to access source data containing single-byte or multibyte character data
- Future needs for single-byte and multibyte data

The data movement mode affects how the PowerCenter Integration Service enforces session code page relationships and code page validation. It can also affect performance. Applications can process single-byte characters faster than multibyte characters.

Character Data Movement Modes

The PowerCenter Integration Service runs in the following modes:

- ASCII (American Standard Code for Information Interchange). The US-ASCII code page contains a set of 7-bit ASCII characters and is a subset of other character sets. When the PowerCenter Integration Service runs in ASCII data movement mode, each character requires one byte.
- Unicode. The universal character-encoding standard that supports all languages. When the PowerCenter Integration Service runs in Unicode data movement mode, it allots up to two bytes for each character. Run the PowerCenter Integration Service in Unicode mode when the source contains multibyte data.

Tip: You can also use ASCII or Unicode data movement mode if the source has 8-bit ASCII data. The PowerCenter Integration Service allots an extra byte when processing data in Unicode data movement mode. To increase performance, use the ASCII data movement mode. For example, if the source contains characters from the ISO 8859-1 code page, use the ASCII data movement.

The data movement you choose affects the requirements for code pages. Ensure the code pages are compatible.

ASCII Data Movement Mode

In ASCII mode, the PowerCenter Integration Service processes single-byte characters and does not perform code page conversions. When you run the PowerCenter Integration Service in ASCII mode, it does not enforce session code page relationships.

Unicode Data Movement Mode

In Unicode mode, the PowerCenter Integration Service recognizes multibyte character data and allocates up to two bytes for every character. The PowerCenter Integration Service performs code page conversions from sources to targets. When you set the PowerCenter Integration Service to Unicode data movement mode, it uses a Unicode character set to process characters in a specified code page, such as Shift-JIS or UTF-8.

When you run the PowerCenter Integration Service in Unicode mode, it enforces session code page relationships.

Changing Data Movement Modes

You can change the data movement mode in the PowerCenter Integration Service properties in the Administrator tool. After you change the data movement mode, the PowerCenter Integration Service runs in the new data movement mode the next time you start the PowerCenter Integration Service. When the data movement mode changes, the PowerCenter Integration Service handles character data differently. To avoid creating data inconsistencies in your target tables, the PowerCenter Integration Service performs additional checks for sessions that reuse session caches and files.

The following table describes how the PowerCenter Integration Service handles session files and caches after you change the data movement mode:

Session File or Cache	Time of Creation or Use	PowerCenter Integration Service Behavior After Data Movement Mode Change
Session Log File (*.log)	Each session.	No change in behavior. Creates a new session log for each session using the code page of the PowerCenter Integration Service process.
Workflow Log	Each workflow.	No change in behavior. Creates a new workflow log file for each workflow using the code page of the PowerCenter Integration Service process.
Reject File (*.bad)	Each session.	No change in behavior. Appends rejected data to the existing reject file using the code page of the PowerCenter Integration Service process.
Output File (*.out)	Sessions writing to flat file.	No change in behavior. Creates a new output file for each session using the target code page.
Indicator File (*.in)	Sessions writing to flat file.	No change in behavior. Creates a new indicator file for each session.

Session File or Cache	Time of Creation or Use	PowerCenter Integration Service Behavior After Data Movement Mode Change
Incremental Aggregation Files (*.idx, *.dat)	Sessions with Incremental Aggregation enabled.	<p>When files are removed or deleted, the PowerCenter Integration Service creates new files.</p> <p>When files are not moved or deleted, the PowerCenter Integration Service fails the session with the following error message:</p> <pre>SM_7038 Aggregate Error: ServerMode: [server data movement mode] and CachedMode: [data movement mode that created the files] mismatch.</pre> <p>Move or delete files created using a different code page.</p>
Unnamed Persistent Lookup Files (*.idx, *.dat)	Sessions with a Lookup transformation configured for an unnamed persistent lookup cache.	Rebuilds the persistent lookup cache.
Named Persistent Lookup Files (*.idx, *.dat)	Sessions with a Lookup transformation configured for a named persistent lookup cache.	<p>When files are removed or deleted, the PowerCenter Integration Service creates new files.</p> <p>When files are not moved or deleted, the PowerCenter Integration Service fails the session.</p> <p>Move or delete files created using a different code page.</p>

Code Page Overview

A code page contains the encoding to specify characters in a set of one or more languages. An encoding is the assignment of a number to a character in the character set. You use code pages to identify data that might be in different languages. For example, if you create a mapping to process Japanese data, you must select a Japanese code page for the source data.

When you choose a code page, the program or application for which you set the code page refers to a specific set of data that describes the characters the application recognizes. This influences the way that application stores, receives, and sends character data.

Most machines use one of the following code pages:

- US-ASCII (7-bit ASCII)
- MS Latin1 (MS 1252) for Windows operating systems
- Latin1 (ISO 8859-1) for UNIX operating systems
- IBM EBCDIC US English (IBM037) for mainframe systems

The US-ASCII code page contains all 7-bit ASCII characters and is the most basic of all code pages with support for United States English. The US-ASCII code page is not compatible with any other code page. When you install either the PowerCenter Client, PowerCenter Integration Service, or PowerCenter repository on a US-ASCII system, you must install all components on US-ASCII systems and run the PowerCenter Integration Service in ASCII mode.

MS Latin1 and Latin1 both support English and most Western European languages and are compatible with each other. When you install the PowerCenter Client, PowerCenter Integration Service, or PowerCenter

repository on a system using one of these code pages, you can install the rest of the components on any machine using the MS Latin1 or Latin1 code pages.

You can use the IBM EBCDIC code page for the PowerCenter Integration Service process when you install it on a mainframe system. You cannot install the PowerCenter Client or PowerCenter repository on mainframe systems, so you cannot use the IBM EBCDIC code page for PowerCenter Client or PowerCenter repository installations.

UNIX Code Pages

In the United States, most UNIX operating systems have more than one code page installed and use the ASCII code page by default. If you want to run PowerCenter in an ASCII-only environment, you can use the ASCII code page and run the PowerCenter Integration Service in ASCII mode.

UNIX systems allow you to change the code page by changing the LANG, LC_CTYPE or LC_ALL environment variable. For example, you want to change the code page an HP-UX machine uses. Use the following command in the C shell to view your environment:

```
locale
```

This results in the following output, in which "C" implies "ASCII":

```
LANG="C"
LC_CTYPE="C"
LC_NUMERIC="C"
LC_TIME="C"
LC_ALL="C"
```

To change the language to English and require the system to use the Latin1 code page, you can use the following command:

```
setenv LANG en_US.iso88591
```

When you check the locale again, it has been changed to use Latin1 (ISO 8859-1):

```
LANG="en_US.iso88591"
LC_CTYPE="en_US.iso88591"
LC_NUMERIC="en_US.iso88591"
LC_TIME="en_US.iso88591"
LC_ALL="en_US.iso88591"
```

For more information about changing the locale or code page of a UNIX system, see the UNIX documentation.

Windows Code Pages

The Windows operating system is based on Unicode, but does not display the code page used by the operating system in the environment settings. However, you can make an educated guess based on the country in which you purchased the system and the language the system uses.

If you purchase Windows in the United States and use English as an input and display language, your operating system code page is MS Latin1 (MS1252) by default. However, if you install additional display or input languages from the Windows installation CD and use those languages, the operating system might use a different code page.

For more information about the default code page for your Windows system, contact Microsoft.

Choosing a Code Page

Choose code pages based on the character data you use in mappings. Character data can be represented by character modes based on the character size. Character size is the storage space a character requires in the database. Different character sizes can be defined as follows:

- Single-byte. A character represented as a unique number between 0 and 255. One byte is eight bits. ASCII characters are single-byte characters.
- Double-byte. A character two bytes or 16 bits in size represented as a unique number 256 or greater. Many Asian languages, such as Chinese, have double-byte characters.
- Multibyte. A character two or more bytes in size is represented as a unique number 256 or greater. Many Asian languages, such as Chinese, have multibyte characters.

Code Page Compatibility

Compatibility between code pages is essential for accurate data movement when the PowerCenter Integration Service runs in the Unicode data movement mode.

A code page can be compatible with another code page, or it can be a subset or a superset of another:

- Compatible. Two code pages are compatible when the characters encoded in the two code pages are virtually identical. For example, JapanEUC and JIPSE code pages contain identical characters and are compatible with each other. The PowerCenter repository and PowerCenter Integration Service process can each use one of these code pages and can pass data back and forth without data loss.
- Superset. A code page is a superset of another code page when it contains all the characters encoded in the other code page and additional characters not encoded in the other code page. For example, MS Latin1 is a superset of US-ASCII because it contains all characters in the US-ASCII code page.

Note: Informatica considers a code page to be a superset of itself and all other compatible code pages.

- Subset. A code page is a subset of another code page when all characters in the code page are also encoded in the other code page. For example, US-ASCII is a subset of MS Latin1 because all characters in the US-ASCII code page are also encoded in the MS Latin1 code page.

For accurate data movement, the target code page must be a superset of the source code page. If the target code page is not a superset of the source code page, the PowerCenter Integration Service may not process all characters, resulting in incorrect or missing data. For example, Latin1 is a superset of US-ASCII. If you select Latin1 as the source code page and US-ASCII as the target code page, you might lose character data if the source contains characters that are not included in US-ASCII.

When you install or upgrade a PowerCenter Integration Service to run in Unicode mode, you must ensure code page compatibility among the domain configuration database, the Administrator tool, PowerCenter Clients, PowerCenter Integration Service process nodes, the PowerCenter repository, the Metadata Manager repository, and the machines hosting *pmrep* and *pmcmd*. In Unicode mode, the PowerCenter Integration Service enforces code page compatibility between the PowerCenter Client and the PowerCenter repository, and between the PowerCenter Integration Service process and the PowerCenter repository. In addition, when you run the PowerCenter Integration Service in Unicode mode, code pages associated with sessions must have the appropriate relationships:

- For each source in the session, the source code page must be a subset of the target code page. The PowerCenter Integration Service does not require code page compatibility between the source and the PowerCenter Integration Service process or between the PowerCenter Integration Service process and the target.

- If the session contains a Lookup or Stored Procedure transformation, the database or file code page must be a subset of the target that receives data from the Lookup or Stored Procedure transformation and a superset of the source that provides data to the Lookup or Stored Procedure transformation.
- If the session contains an External Procedure or Custom transformation, the procedure must pass data in a code page that is a subset of the target code page for targets that receive data from the External Procedure or Custom transformation.

Informatica uses code pages for the following components:

- Domain configuration database. The domain configuration database must be compatible with the code pages of the PowerCenter repository and Metadata Manager repository.
- Administrator tool. You can enter data in any language in the Administrator tool.
- PowerCenter Client. You can enter metadata in any language in the PowerCenter Client.
- PowerCenter Integration Service process. The PowerCenter Integration Service can move data in ASCII mode and Unicode mode. The default data movement mode is ASCII, which passes 7-bit ASCII or 8-bit ASCII character data. To pass multibyte character data from sources to targets, use the Unicode data movement mode. When you run the PowerCenter Integration Service in Unicode mode, it uses up to three bytes for each character to move data and performs additional checks at the session level to ensure data integrity.
- PowerCenter repository. The PowerCenter repository can store data in any language. You can use the UTF-8 code page for the PowerCenter repository to store multibyte data in the PowerCenter repository. The code page for the PowerCenter repository is the same as the database code page.
- Metadata Manager repository. The Metadata Manager repository can store data in any language. You can use the UTF-8 code page for the Metadata Manager repository to store multibyte data in the repository. The code page for the repository is the same as the database code page.
- Sources and targets. The sources and targets store data in one or more languages. You use code pages to specify the type of characters in the sources and targets.
- PowerCenter command line programs. You must also ensure that the code page for *pmrep* is a subset of the PowerCenter repository code page and the code page for *pmcmd* is a subset of the PowerCenter Integration Service process code page.

Most database servers use two code pages, a client code page to receive data from client applications and a server code page to store the data. When the database server is running, it converts data between the two code pages if they are different. In this type of database configuration, the PowerCenter Integration Service process interacts with the database client code page. Thus, code pages used by the PowerCenter Integration Service process, such as the PowerCenter repository, source, or target code pages, must be identical to the database client code page. The database client code page is usually identical to the operating system code page on which the PowerCenter Integration Service process runs. The database client code page is a subset of the database server code page.

For more information about specific database client and server code pages, see your database documentation.

Note: The Reporting Service does not require that you specify a code page for the data that is stored in the Data Analyzer repository. The Administrator tool writes domain, user, and group information to the Reporting Service. However, DataDirect drivers perform the required data conversions.

Domain Configuration Database Code Page

The domain configuration database must be compatible with the code pages of the PowerCenter repository, Metadata Manager repository, and Model repository.

The Service Manager synchronizes the list of users in the domain with the list of users and groups in each application service. If a user name in the domain has characters that the code page of the application service does not recognize, characters do not convert correctly and inconsistencies occur.

Administrator Tool Code Page

The Administrator tool can run on any node in a Informatica domain. The Administrator tool code page is the code page of the operating system of the node. Each node in the domain must use the same code page.

The Administrator tool code page must be:

- A subset of the PowerCenter repository code page
- A subset of the Metadata Manager repository code page
- A subset of the Model Repository code page

PowerCenter Client Code Page

The PowerCenter Client code page is the code page of the operating system of the PowerCenter Client. To communicate with the PowerCenter repository, the PowerCenter Client code page must be a subset of the PowerCenter repository code page.

PowerCenter Integration Service Process Code Page

The code page of a PowerCenter Integration Service process is the code page of the node that runs the PowerCenter Integration Service process. Define the code page for each PowerCenter Integration Service process in the Administrator tool on the Processes tab.

However, on UNIX, you can change the code page of the PowerCenter Integration Service process by changing the LANG, LC_CTYPE or LC_ALL environment variable for the user that starts the process.

The code page of the PowerCenter Integration Service process must be:

- A subset of the PowerCenter repository code page
- A superset of the machine hosting *pmcmd* or a superset of the code page specified in the INFA_CODEPAGENAME environment variable

The code pages of all PowerCenter Integration Service processes must be compatible with each other. For example, you can use MS Windows Latin1 for a node on Windows and ISO-8859-1 for a node on UNIX.

PowerCenter Integration Services configured for Unicode mode validate code pages when you start a session to ensure accurate data movement. It uses session code pages to convert character data. When the PowerCenter Integration Service runs in ASCII mode, it does not validate session code pages. It reads all character data as ASCII characters and does not perform code page conversions.

Each code page has associated sort orders. When you configure a session, you can select one of the sort orders associated with the code page of the PowerCenter Integration Service process. When you run the PowerCenter Integration Service in Unicode mode, it uses the selected session sort order to sort character data. When you run the PowerCenter Integration Service in ASCII mode, it sorts all character data using a binary sort order.

If you run the PowerCenter Integration Service in the United States on Windows, consider using MS Windows Latin1 (ANSI) as the code page of the PowerCenter Integration Service process.

If you run the PowerCenter Integration Service in the United States on UNIX, consider using ISO 8859-1 as the code page for the PowerCenter Integration Service process.

If you use *pmcmd* to communicate with the PowerCenter Integration Service, the code page of the operating system hosting *pmcmd* must be identical to the code page of the PowerCenter Integration Service process.

The PowerCenter Integration Service generates the names of session log files, reject files, caches and cache files, and performance detail files based on the code page of the PowerCenter Integration Service process.

PowerCenter Repository Code Page

The PowerCenter repository code page is the code page of the data in the repository. The PowerCenter Repository Service uses the PowerCenter repository code page to save metadata in and retrieve metadata from the PowerCenter repository database. Choose the PowerCenter repository code page when you create or upgrade a PowerCenter repository. When the PowerCenter repository database code page is UTF-8, you can create a PowerCenter repository using UTF-8 as its code page.

The PowerCenter repository code page must be:

- Compatible with the domain configuration database code page
- A superset of the the Administrator tool code page
- A superset of the PowerCenter Client code page
- A superset of the code page for the PowerCenter Integration Service process
- A superset of the machine hosting *pmrep* or a superset of the code page specified in the INFA_CODEPAGE environment variable

A global PowerCenter repository code page must be a subset of the local PowerCenter repository code page if you want to create shortcuts in the local PowerCenter repository that reference an object in a global PowerCenter repository.

If you copy objects from one PowerCenter repository to another PowerCenter repository, the code page for the target PowerCenter repository must be a superset of the code page for the source PowerCenter repository.

Metadata Manager Repository Code Page

The Metadata Manager repository code page is the code page of the data in the repository. The Metadata Manager Service uses the Metadata Manager repository code page to save metadata to and retrieve metadata from the repository database. The Administrator tool writes user and group information to the Metadata Manager Service. The Administrator tool also writes domain information in the repository database. The PowerCenter Integration Service process writes metadata to the repository database. Choose the repository code page when you create or upgrade a Metadata Manager repository. When the repository database code page is UTF-8, you can create a repository using UTF-8 as its code page.

The Metadata Manager repository code page must be:

- Compatible with the domain configuration database code page
- A superset of the Administrator tool code page
- A subset of the PowerCenter repository code page
- A superset of the code page for the PowerCenter Integration Service process

PowerCenter Source Code Page

The source code page depends on the type of source:

- Flat files and VSAM files. The code page of the data in the file. When you configure the flat file or COBOL source definition, choose a code page that matches the code page of the data in the file.

- XML files. The PowerCenter Integration Service converts XML to Unicode when it parses an XML source. When you create an XML source definition, the PowerCenter Designer assigns a default code page. You cannot change the code page.
- Relational databases. The code page of the database client. When you configure the relational connection in the PowerCenter Workflow Manager, choose a code page that is compatible with the code page of the database client. If you set a database environment variable to specify the language for the database, ensure the code page for the connection is compatible with the language set for the variable. For example, if you set the NLS_LANG environment variable for an Oracle database, ensure that the code page of the Oracle connection is identical to the value set in the NLS_LANG variable. If you do not use compatible code pages, sessions may hang, data may become inconsistent, or you might receive a database error, such as:

ORA-00911: Invalid character specified.

Regardless of the type of source, the source code page must be a subset of the code page of transformations and targets that receive data from the source. The source code page does not need to be a subset of transformations or targets that do not receive data from the source.

Note: Select IBM EBCDIC as the source database connection code page only if you access EBCDIC data, such as data from a mainframe extract file.

PowerCenter Target Code Page

The target code page depends on the type of target:

- Flat files. When you configure the flat file target definition, choose a code page that matches the code page of the data in the flat file.
- XML files. Configure the XML target code page after you create the XML target definition. The XML Wizard assigns a default code page to the XML target. The PowerCenter Designer does not apply the code page that appears in the XML schema.
- Relational databases. When you configure the relational connection in the PowerCenter Workflow Manager, choose a code page that is compatible with the code page of the database client. If you set a database environment variable to specify the language for the database, ensure the code page for the connection is compatible with the language set for the variable. For example, if you set the NLS_LANG environment variable for an Oracle database, ensure that the code page of the Oracle connection is compatible with the value set in the NLS_LANG variable. If you do not use compatible code pages, sessions may hang or you might receive a database error, such as:

ORA-00911: Invalid character specified.

The target code page must be a superset of the code page of transformations and sources that provide data to the target. The target code page does not need to be a superset of transformations or sources that do not provide data to the target.

The PowerCenter Integration Service creates session indicator files, session output files, and external loader control and data files using the target flat file code page.

Note: Select IBM EBCDIC as the target database connection code page only if you access EBCDIC data, such as data from a mainframe extract file.

Command Line Program Code Pages

The *pmcmd* and *pmrep* command line programs require code page compatibility. *pmcmd* and *pmrep* use code pages when sending commands in Unicode. Other command line programs do not require code pages.

The code page compatibility for *pmcmd* and *pmrep* depends on whether you configured the code page environment variable `INFA_CODEPAGENAME` for *pmcmd* or *pmrep*. You can set this variable for either command line program or for both.

If you did not set this variable for a command line program, ensure the following requirements are met:

- If you did not set the variable for *pmcmd*, then the code page of the machine hosting *pmcmd* must be a subset of the code page for the PowerCenter Integration Service process.
- If you did not set the variable for *pmrep*, then the code page of the machine hosting *pmrep* must be a subset of the PowerCenter repository code page.

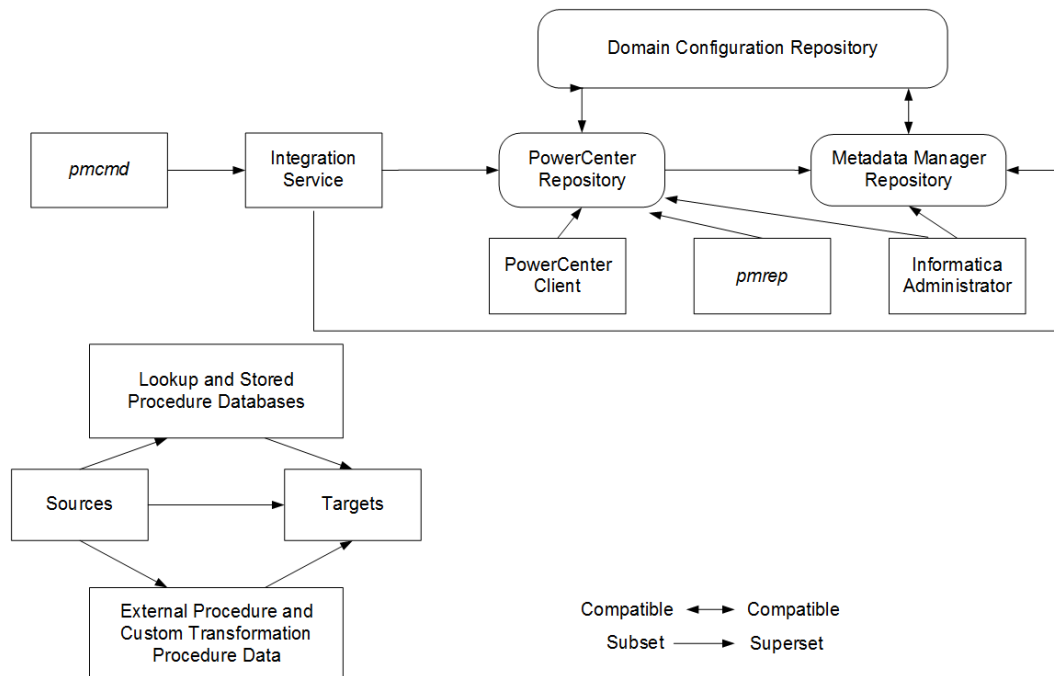
If you set the code page environment variable `INFA_CODEPAGENAME` for *pmcmd* or *pmrep*, ensure the following requirements are met:

- If you set `INFA_CODEPAGENAME` for *pmcmd*, the code page defined for the variable must be a subset of the code page for the PowerCenter Integration Service process.
- If you set `INFA_CODEPAGENAME` for *pmrep*, the code page defined for the variable must be a subset of the PowerCenter repository code page.
- If you run *pmcmd* and *pmrep* from the same machine and you set the `INFA_CODEPAGENAME` variable, the code page defined for the variable must be subsets of the code pages for the PowerCenter Integration Service process and the PowerCenter repository.

If the code pages are not compatible, the PowerCenter Integration Service process may not fetch the workflow, session, or task from the PowerCenter repository.

Code Page Compatibility Summary

The following image shows code page compatibility in the Informatica environment:



The following table summarizes code page compatibility between sources, targets, repositories, the Informatica Administrator, PowerCenter Client, and Integration Service process:

Component Code Page	Code Page Compatibility
Source (including relational, flat file, and XML file)	Subset of target. Subset of lookup data. Subset of stored procedures. Subset of External Procedure or Custom transformation procedure code page.
Target (including relational, XML files, and flat files)	Superset of source. Superset of lookup data. Superset of stored procedures. Superset of External Procedure or Custom transformation procedure code page. Integration Service process creates external loader data and control files using the target flat file code page.
Lookup and stored procedure database	Subset of target. Superset of source.
External Procedure and Custom transformation procedures	Subset of target. Superset of source.
Domain Configuration Database	Compatible with the PowerCenter Repository Service. Compatible with the Metadata Manager repository.
PowerCenter Integration Service process	Compatible with its operating system. Subset of the PowerCenter repository. Subset of the Metadata Manager repository. Superset of the machine hosting <i>pmcmd</i> . Identical to other nodes running the PowerCenter Integration Service processes.
PowerCenter repository	Compatible with the domain configuration database. Superset of PowerCenter Client. Superset of the nodes running the PowerCenter Integration Service process. Superset of the Metadata Manager repository. A global PowerCenter repository code page must be a subset of a local PowerCenter repository.
PowerCenter Client	Subset of the PowerCenter repository.
Machine running <i>pmcmd</i>	Subset of the PowerCenter Integration Service process.
Machine running <i>pmrep</i>	Subset of the PowerCenter repository.

Component Code Page	Code Page Compatibility
Administrator Tool	Subset of the PowerCenter repository. Subset of the Metadata Manager repository.
Metadata Manager repository	Compatible with the domain configuration database. Subset of the PowerCenter repository. Superset of the Administrator tool. Superset of the PowerCenter Integration Service process.

Code Page Validation

The machines hosting the PowerCenter Client, PowerCenter Integration Service process, and PowerCenter repository database must use appropriate code pages. This eliminates the risk of data or repository inconsistencies. When the PowerCenter Integration Service runs in Unicode data movement mode, it enforces session code page relationships. When the PowerCenter Integration Service runs in ASCII mode, it does not enforce session code page relationships.

To ensure compatibility, the PowerCenter Client and PowerCenter Integration Service perform the following code page validations:

- PowerCenter restricts the use of EBCDIC-based code pages for repositories. Since you cannot install the PowerCenter Client or PowerCenter repository on mainframe systems, you cannot select EBCDIC-based code pages, like IBM EBCDIC, as the PowerCenter repository code page.
- PowerCenter Client can connect to the PowerCenter repository when its code page is a subset of the PowerCenter repository code page. If the PowerCenter Client code page is not a subset of the PowerCenter repository code page, the PowerCenter Client fails to connect to the PowerCenter repository code page with the following error:

```
REP_61082 <PowerCenter Client>'s code page <PowerCenter Client code page> is not one-way compatible to repository <PowerCenter repository name>'s code page <PowerCenter repository code page>.
```

- After you set the PowerCenter repository code page, you cannot change it. After you create or upgrade a PowerCenter repository, you cannot change the PowerCenter repository code page. This prevents data loss and inconsistencies in the PowerCenter repository.
- The PowerCenter Integration Service process can start if its code page is a subset of the PowerCenter repository code page. The code page of the PowerCenter Integration Service process must be a subset of the PowerCenter repository code page to prevent data loss or inconsistencies. If it is not a subset of the PowerCenter repository code page, the PowerCenter Integration Service writes the following message to the log files:

```
REP_61082 <PowerCenter Integration Service>'s code page <PowerCenter Integration Service code page> is not one-way compatible to repository <PowerCenter repository name>'s code page <PowerCenter repository code page>.
```

- When in Unicode data movement mode, the PowerCenter Integration Service starts workflows with the appropriate source and target code page relationships for each session. When the PowerCenter Integration Service runs in Unicode mode, the code page for every source in a session must be a subset of the target code page. This prevents data loss during a session.

If the source and target code pages do not have the appropriate relationships with each other, the PowerCenter Integration Service fails the session and writes the following message to the session log:

```
TM_6227 Error: Code page incompatible in session <session name>. <Additional details>.
```

- The PowerCenter Workflow Manager validates source, target, lookup, and stored procedure code page relationships for each session. The PowerCenter Workflow Manager checks code page relationships when you save a session, regardless of the PowerCenter Integration Service data movement mode. If you configure a session with invalid source, target, lookup, or stored procedure code page relationships, the PowerCenter Workflow Manager issues a warning similar to the following when you save the session:

```
CMN_1933 Code page <code page name> for data from file or connection associated with transformation <name of source, target, or transformation> needs to be one-way compatible with code page <code page name> for transformation <source or target or transformation name>.
```

If you want to run the session in ASCII mode, you can save the session as configured. If you want to run the session in Unicode mode, edit the session to use appropriate code pages.

Relaxed Code Page Validation

Your environment may require you to process data from different sources using character sets from different languages. For example, you may need to process data from English and Japanese sources using the same PowerCenter repository, or you may want to extract source data encoded in a Unicode encoding such as UTF-8. You can configure the PowerCenter Integration Service for relaxed code page validation. Relaxed code page validation enables you to process data using sources and targets with incompatible code pages.

Although relaxed code page validation removes source and target code page restrictions, it still enforces code page compatibility between the PowerCenter Integration Service and PowerCenter repository.

Note: Relaxed code page validation does not safeguard against possible data inconsistencies when you move data between incompatible code pages. You must verify that the characters the PowerCenter Integration Service reads from the source are included in the target code page.

Informatica removes the following restrictions when you relax code page validation:

- Source and target code pages. You can use any code page supported by Informatica for your source and target data.
- Session sort order. You can use any sort order supported by Informatica when you configure a session.

When you run a session with relaxed code page validation, the PowerCenter Integration Service writes the following message to the session log:

```
TM_6185 WARNING! Data code page validation is disabled in this session.
```

When you relax code page validation, the PowerCenter Integration Service writes descriptions of the database connection code pages to the session log.

The following text shows sample code page messages in the session log:

```
TM_6187 Repository code page: [MS Windows Latin 1 (ANSI), superset of Latin 1]
WRT_8222 Target file [$PMTargetFileDir\passthru.out] code page: [MS Windows Traditional Chinese, superset of Big 5]
WRT_8221 Target database connection [Japanese Oracle] code page: [MS Windows Japanese, superset of Shift-JIS]
TM_6189 Source database connection [Japanese Oracle] code page: [MS Windows Japanese, superset of Shift-JIS]
CMN_1716 Lookup [LKP_sjis_lookup] uses database connection [Japanese Oracle] in code page [MS Windows Japanese, superset of Shift-JIS]
CMN_1717 Stored procedure [J_SP_INCREMENT] uses database connection [Japanese Oracle] in code page [MS Windows Japanese, superset of Shift-JIS]
```

If the PowerCenter Integration Service cannot correctly convert data, it writes an error message to the session log.

Configuring the PowerCenter Integration Service

To configure the PowerCenter Integration Service for code page relaxation, complete the following tasks in the Administrator tool:

- Disable code page validation. Disable the ValidateDataCodePages option in the PowerCenter Integration Service properties.
- Configure the PowerCenter Integration Service for Unicode data movement mode. Select Unicode for the Data Movement Mode option in the PowerCenter Integration Service properties.
- Configure the PowerCenter Integration Service to write to the logs using the UTF-8 character set. If you configure sessions or workflows to write to log files, enable the LogsInUTF8 option in the PowerCenter Integration Service properties. The PowerCenter Integration Service writes all logs in UTF-8 when you enable the LogsInUTF8 option. The PowerCenter Integration Service writes to the Log Manager in UTF-8 by default.

Selecting Compatible Source and Target Code Pages

Although PowerCenter allows you to use any supported code page, there are risks associated with using incompatible code pages for sources and targets. If your target code page is not a superset of your source code page, you risk inconsistencies in the target data because the source data may contain characters not encoded in the target code page.

When the PowerCenter Integration Service reads characters that are not included in the target code page, you risk transformation errors, inconsistent data, or failed sessions.

Note: If you relax code page validation, it is your responsibility to ensure that data converts from the source to target properly.

Troubleshooting for Code Page Relaxation

The PowerCenter Integration Service failed a session and wrote the following message to the session log:

```
TM_6188 The specified sort order is incompatible with the PowerCenter Integration
Service code page.
```

If you want to validate code pages, select a sort order compatible with the PowerCenter Integration Service code page. If you want to relax code page validation, configure the PowerCenter Integration Service to relax code page validation in Unicode data movement mode.

[I tried to view the session or workflow log, but it contains garbage characters.](#)

The PowerCenter Integration Service is not configured to write session or workflow logs using the UTF-8 character set.

Enable the LogsInUTF8 option in the PowerCenter Integration Service properties.

PowerCenter Code Page Conversion

When in data movement mode is set to Unicode, the PowerCenter Client accepts input in any language and converts it to UCS-2. The PowerCenter Integration Service converts source data to UCS-2 before processing and converts the processed data from UCS-2 to the target code page before loading.

When you run a session, the PowerCenter Integration Service converts source, target, and lookup queries from the PowerCenter repository code page to the source, target, or lookup code page. The PowerCenter Integration Service also converts the name and call text of stored procedures from the PowerCenter repository code page to the stored procedure database code page.

At run time, the PowerCenter Integration Service verifies that it can convert the following queries and procedure text from the PowerCenter repository code page without data loss:

- Source query. Must convert to source database code page.
- Lookup query. Must convert to lookup database code page.
- Target SQL query. Must convert to target database code page.
- Name and call text of stored procedures. Must convert to stored procedure database code page.

Choosing Characters for PowerCenter Repository Metadata

You can use any character in the PowerCenter repository code page when inputting PowerCenter repository metadata. If the PowerCenter repository uses UTF-8, you can input any Unicode character. For example, you can store German, Japanese, and English metadata in a UTF-8 enabled PowerCenter repository. However, you must ensure that the PowerCenter Integration Service can successfully perform SQL transactions with source, target, lookup, and stored procedure databases. You must also ensure that the PowerCenter Integration Service can read from source and lookup files and write to target and lookup files. Therefore, when you run a session, you must ensure that the PowerCenter repository metadata characters are encoded in the source, target, lookup, and stored procedure code pages.

Example

The PowerCenter Integration Service, PowerCenter repository, and PowerCenter Client use the ISO 8859-1 Latin1 code page, and the source database contains Japanese data encoded using the Shift-JIS code page. Each code page contains characters not encoded in the other. Using characters other than 7-bit ASCII for the PowerCenter repository and source database metadata can cause the sessions to fail or load no rows to the target in the following situations:

- You create a mapping that contains a string literal with characters specific to the German language range of ISO 8859-1 in a query. The source database may reject the query or return inconsistent results.
- You use the PowerCenter Client to generate SQL queries containing characters specific to the German language range of ISO 8859-1. The source database cannot convert the German-specific characters from the ISO 8859-1 code page into the Shift-JIS code page.
- The source database has a table name that contains Japanese characters. The PowerCenter Designer cannot convert the Japanese characters from the source database code page to the PowerCenter Client code page. Instead, the PowerCenter Designer imports the Japanese characters as question marks (?), changing the name of the table. The PowerCenter Repository Service saves the source table name in the PowerCenter repository as question marks. If the PowerCenter Integration Service sends a query to the source database using the changed table name, the source database cannot find the correct table, and returns no rows or an error to the PowerCenter Integration Service, causing the session to fail.

Because the US-ASCII code page is a subset of both the ISO 8859-1 and Shift-JIS code pages, you can avoid these data inconsistencies if you use 7-bit ASCII characters for all of your metadata.

Case Study: Processing ISO 8859-1 Data

This case study describes how you might set up an environment to process ISO 8859-1 multibyte data. You might want to configure your environment this way if you need to process data from different Western European languages with character sets contained in the ISO 8859-1 code page. This example describes an environment that processes English and German language data.

For this case study, the ISO 8859-1 environment consists of the following elements:

- The PowerCenter Integration Service on a UNIX system
- PowerCenter Client on a Windows system, purchased in the United States
- The PowerCenter repository stored on an Oracle database on UNIX
- A source database containing English language data
- Another source database containing German and English language data
- A target database containing German and English language data
- A lookup database containing English language data

The data environment must process English and German character data.

The ISO 8859-1 Environment

The data environment must process English and German character data.

Configuring the ISO 8859-1 Environment

Use the following guidelines when you configure an environment similar to this case study for ISO 8859-1 data processing:

1. Verify code page compatibility between the PowerCenter repository database client and the database server.
2. Verify code page compatibility between the PowerCenter Client and the PowerCenter repository, and between the PowerCenter Integration Service process and the PowerCenter repository.
3. Set the PowerCenter Integration Service data movement mode to ASCII.
4. Verify session code page compatibility.
5. Verify lookup and stored procedure database code page compatibility.
6. Verify External Procedure or Custom transformation procedure code page compatibility.
7. Configure session sort order.

Step 1. Verify PowerCenter Repository Database Client and Server Compatibility

The database client and server hosting the PowerCenter repository must be able to communicate without data loss.

The PowerCenter repository resides in an Oracle database. Use `NLS_LANG` to set the locale (language, territory, and character set) you want the database client and server to use with your login:

```
NLS_LANG = LANGUAGE_TERRITORY.CHARACTERSET
```

By default, Oracle configures NLS_LANG for the U.S. English language, the U.S. territory, and the 7-bit ASCII character set:

```
NLS_LANG = AMERICAN_AMERICA.US7ASCII
```

Change the default configuration to write ISO 8859-1 data to the PowerCenter repository using the Oracle WE8ISO8859P1 code page. For example:

```
NLS_LANG = AMERICAN_AMERICA.WE8ISO8859P1
```

For more information about verifying and changing the PowerCenter repository database code page, see your database documentation.

Step 2. Verify PowerCenter Code Page Compatibility

The PowerCenter Integration Service and PowerCenter Client code pages must be subsets of the PowerCenter repository code page. Because the PowerCenter Client and PowerCenter Integration Service each use the system code pages of the machines they are installed on, you must verify that the system code pages are subsets of the PowerCenter repository code page.

In this case, the PowerCenter Client on Windows systems were purchased in the United States. Thus the system code pages for the PowerCenter Client machines are set to MS Windows Latin1 by default. To verify system input and display languages, open the Regional Options dialog box from the Windows Control Panel. For systems purchased in the United States, the Regional Settings and Input Locale must be configured for English (United States).

The PowerCenter Integration Service is installed on a UNIX machine. The default code page for UNIX operating systems is ASCII. In this environment, change the UNIX system code page to ISO 8859-1 Western European so that it is a subset of the PowerCenter repository code page.

Step 3. Configure the PowerCenter Integration Service for ASCII Data Movement Mode

Configure the PowerCenter Integration Service to process ISO 8859-1 data. In the Administrator tool, set the Data Movement Mode to ASCII for the PowerCenter Integration Service.

Step 4. Verify Session Code Page Compatibility

When you run a workflow in ASCII data movement mode, the PowerCenter Integration Service enforces source and target code page relationships. To guarantee accurate data conversion, the source code page must be a subset of the target code page.

In this case, the environment contains source databases containing German and English data. When you configure a source database connection in the PowerCenter Workflow Manager, the code page for the connection must be identical to the source database code page and must be a subset of the target code page. Since both the MS Windows Latin1 and the ISO 8859-1 Western European code pages contain German characters, you would most likely use one of these code pages for source database connections.

Because the target code page must be a superset of the source code page, use either MS Windows Latin1, ISO 8859-1 Western European, or UTF-8 for target database connection or flat file code pages. To ensure data consistency, the configured target code page must match the target database or flat file system code page.

If you configure the PowerCenter Integration Service for relaxed code page validation, the PowerCenter Integration Service removes restrictions on source and target code page compatibility. You can select any supported code page for source and target data. However, you must ensure that the targets only receive character data encoded in the target code page.

Step 5. Verify Lookup and Stored Procedure Database Code Page Compatibility

Lookup and stored procedure database code pages must be supersets of the source code pages and subsets of the target code pages. In this case, all lookup and stored procedure database connections must use a code page compatible with the ISO 8859-1 Western European or MS Windows Latin1 code pages.

Step 6. Verify External Procedure or Custom Transformation Procedure Compatibility

External Procedure and Custom transformation procedures must be able to process character data from the source code pages, and they must pass characters that are compatible in the target code pages. In this case, all data processed by the External Procedure or Custom transformations must be in the ISO 8859-1 Western European or MS Windows Latin1 code pages.

Step 7. Configure Session Sort Order

When you run the PowerCenter Integration Service in ASCII mode, it uses a binary sort order for all sessions. In the session properties, the PowerCenter Workflow Manager lists all sort orders associated with the PowerCenter Integration Service code page. You can select a sort order for the session.

Case Study: Processing Unicode UTF-8 Data

This case study describes how you might set up an environment that processes Unicode UTF-8 multibyte data. You might want to configure your environment this way if you need to process data from Western European, Middle Eastern, Asian, or any other language with characters encoded in the UTF-8 character set. This example describes an environment that processes German and Japanese language data.

For this case study, the UTF-8 environment consists of the following elements:

- The PowerCenter Integration Service on a UNIX machine
 - The PowerCenter Clients on Windows systems
 - The PowerCenter repository stored on an Oracle database on UNIX
 - A source database contains German language data
 - A source database contains German and Japanese language data
 - A target database contains German and Japanese language data
 - A lookup database contains German language data
- The data environment must process German and Japanese character data.

The UTF-8 Environment

The data environment must process German and Japanese character data.

Configuring the UTF-8 Environment

Use the following guidelines when you configure an environment similar to this case study for UTF-8 data processing:

1. Verify code page compatibility between the PowerCenter repository database client and the database server.
2. Verify code page compatibility between the PowerCenter Client and the PowerCenter repository, and between the PowerCenter Integration Service and the PowerCenter repository.
3. Configure the PowerCenter Integration Service for Unicode data movement mode.
4. Verify session code page compatibility.
5. Verify lookup and stored procedure database code page compatibility.
6. Verify External Procedure or Custom transformation procedure code page compatibility.
7. Configure session sort order.

Step 1. Verify PowerCenter Repository Database Client and Server Code Page Compatibility

The database client and server hosting the PowerCenter repository must be able to communicate without data loss.

The PowerCenter repository resides in an Oracle database. With Oracle, you can use `NLS_LANG` to set the locale (language, territory, and character set) you want the database client and server to use with your login:

```
NLS_LANG = LANGUAGE_TERRITORY.CHARACTERSET
```

By default, Oracle configures `NLS_LANG` for U.S. English language, the U.S. territory, and the 7-bit ASCII character set:

```
NLS_LANG = AMERICAN_AMERICA.US7ASCII
```

Change the default configuration to write UTF-8 data to the PowerCenter repository using the Oracle UTF8 character set. For example:

```
NLS_LANG = AMERICAN_AMERICA.UTF8
```

For more information about verifying and changing the PowerCenter repository database code page, see your database documentation.

Step 2. Verify PowerCenter Code Page Compatibility

The PowerCenter Integration Service and PowerCenter Client code pages must be subsets of the PowerCenter repository code page. Because the PowerCenter Client and PowerCenter Integration Service each use the system code pages of the machines they are installed on, you must verify that the system code pages are subsets of the PowerCenter repository code page.

In this case, the PowerCenter Client on Windows systems were purchased in Switzerland. Thus, the system code pages for the PowerCenter Client machines are set to MS Windows Latin1 by default. To verify system input and display languages, open the Regional Options dialog box from the Windows Control Panel.

The PowerCenter Integration Service is installed on a UNIX machine. The default code page for UNIX operating systems is ASCII. In this environment, the UNIX system character set must be changed to UTF-8.

Step 3. Configure the PowerCenter Integration Service for Unicode Data Movement Mode

You must configure the PowerCenter Integration Service to process UTF-8 data. In the Administrator tool, set the Data Movement Mode to Unicode for the PowerCenter Integration Service. The PowerCenter Integration Service allots an extra byte for each character when processing multibyte data.

Step 4. Verify Session Code Page Compatibility

When you run a PowerCenter workflow in Unicode data movement mode, the PowerCenter Integration Service enforces source and target code page relationships. To guarantee accurate data conversion, the source code page must be a subset of the target code page.

In this case, the environment contains a source database containing German and Japanese data. When you configure a source database connection in the PowerCenter Workflow Manager, the code page for the connection must be identical to the source database code page. You can use any code page for the source database.

Because the target code page must be a superset of the source code pages, you must use UTF-8 for the target database connections or flat files. To ensure data consistency, the configured target code page must match the target database or flat file system code page.

If you configure the PowerCenter Integration Service for relaxed code page validation, the PowerCenter Integration Service removes restrictions on source and target code page compatibility. You can select any supported code page for source and target data. However, you must ensure that the targets only receive character data encoded in the target code page.

Step 5. Verify Lookup and Stored Procedure Database Code Page Compatibility

Lookup and stored procedure database code pages must be supersets of the source code pages and subsets of the target code pages. In this case, all lookup and stored procedure database connections must use a code page compatible with UTF-8.

Step 6. Verify External Procedure or Custom Transformation Procedure Compatibility

External Procedure and Custom transformation procedures must be able to process character data from the source code pages, and they must pass characters that are compatible in the target code pages.

In this case, the External Procedure or Custom transformations must be able to process the German and Japanese data from the sources. However, the PowerCenter Integration Service passes data to procedures in UCS-2. Therefore, all data processed by the External Procedure or Custom transformations must be in the UCS-2 character set.

Step 7. Configure Session Sort Order

When you run the PowerCenter Integration Service in Unicode mode, it sorts session data using the sort order configured for the session. By default, sessions are configured for a binary sort order.

To sort German and Japanese data when the PowerCenter Integration Service uses UTF-8, you most likely want to use the default binary sort order.

CHAPTER 15

Informatica Cloud Administration

This chapter includes the following topics:

- [Informatica Cloud Administration Overview , 242](#)
- [Informatica Cloud Organizations , 242](#)
- [Informatica Cloud Secure Agent, 244](#)
- [Informatica Cloud Connections, 244](#)

Informatica Cloud Administration Overview

If you use Informatica Cloud, you can add the details of your Informatica Cloud organization to the Administrator tool.

You can view the details of the organizations in the **Cloud** tab. You must have sufficient privileges to view the **Cloud** tab.

You can add or remove organizations in the Administrator tool. After you add a organization, you can view the Secure Agents and Informatica Cloud connections in the organization. A Secure Agent is a lightweight program that runs all tasks and enables secure communication across the firewall between your company and Informatica Cloud. Informatica Cloud connections are the connections that users create in the organization to access data in different data sources.

You can monitor the status of Secure Agents and view the properties of organizations, Secure Agents, and connections. You cannot make any changes to organizations, Secure Agents, or connections from the Administrator tool.

Informatica Cloud Organizations

An Informatica Cloud Organization is a secure area within the Informatica Cloud repository where you store information and objects.

Your company might create multiple organizations based on requirements. For example, the Informatica Cloud Administrator might create a sandbox organization and a production organization. An organization can also have multiple sub-organizations. In the Administrator tool, you can add organizations to view properties of organizations, Secure Agents, and connections and monitor the status of Secure Agents.

You cannot modify any property of the organization from the Administrator tool.

Note: If the organization credentials expire or if there is any issue with connectivity to Informatica Cloud, the organization name appears as "Unidentified."

Informatica Cloud Organization Properties

In the Administrator tool, you can view properties of organizations.

You can view the following details of an organization:

Organization details

The details of the organization such as name and address.

Organization properties

The properties associated with the organization such as creation date and organization ID.

Default email notification options

Default email addresses to receive notifications on jobs.

Authentication options

The details of the authentication used by the organization.

Sub-organizations

The list of sub-organizations associated with the organization.

Adding an Organization

To add an organization in the Administration tool, you must have the sufficient privileges.

1. Click the **Cloud** tab.
2. From the **Actions** menu, choose **Add Organization**.
3. Enter the username and password of the Informatica Cloud organization.
The Informatica Cloud user must have administrator privileges in the organization.
4. Click **OK**.

Removing an Organization

You can remove an organization if you have the sufficient privileges.

1. Click the **Cloud** tab.
2. From the **Actions** menu, choose **Remove Organization**.
The **Remove Organization** dialog box appears.
3. Click **Yes**.

Editing Informatica Cloud Login Credentials

You can update the Informatica Cloud login credentials of an organization to use new login credentials or if the existing login credentials expire.

1. Click the **Cloud** tab.
2. Select the organization.
3. From the **Actions** menu, choose **Edit Login**.

The **Edit Login Credentials** dialog box appears.

4. Select **Modify Password** to update the password.
5. Enter the new login credentials.
6. Click **OK**.

Informatica Cloud Secure Agent

The Informatica Cloud Secure Agent is a lightweight program that runs all tasks and enables secure communication across the firewall between your organization and Informatica Cloud.

After you add an organization in the Administrator tool, you can view the Secure Agents associated with the organization. You can monitor the status of Secure Agents and initiate appropriate actions through Informatica Cloud. You can also view the properties of a Secure Agent.

In the navigator of the **Cloud** tab, expand an organization and select **Secure Agents** to view the list of Secure Agents.

You can view the following details of a Secure Agent in the Administrator tool:

- Secure Agent details
- Secure Agent version details
- Package details
- Secure Agent configuration details
- Other properties

Informatica Cloud Connections

An Informatica Cloud connection is an Informatica Cloud object that you configure to connect to cloud and on-premise applications, platforms, databases, and flat files.

After you add an organization in the Administrator tool, you can view the connections that you configured for the organization in Informatica Cloud.

In the navigator of the **Cloud** tab, expand an organization and select **Connections** to view the list of connections on the right pane.

You can view the following details of a cloud connection in the Administrator tool:

- Connection details
- Connection properties

APPENDIX A

Code Pages

This appendix includes the following topics:

- [Supported Code Pages for Application Services, 245](#)
- [Supported Code Pages for Sources and Targets, 247](#)

Supported Code Pages for Application Services

Informatica supports code pages for internationalization. Informatica uses International Components for Unicode (ICU) for its globalization support. For a list of code page aliases in ICU, see <http://demo.icu-project.org/icu-bin/convexp>.

When you assign an application service code page in the Administrator tool, you select the code page description.

You must use UTF-8 compatible code pages for the domain, Model Repository Service, and for each Data Integration Service process.

The following table lists the name, description, and ID for supported code pages for the PowerCenter Repository Service, the Metadata Manager Service, and for each PowerCenter Integration Service process:

Name	Description	ID
IBM037	IBM EBCDIC US English	2028
IBM1047	IBM EBCDIC US English IBM1047	1047
IBM273	IBM EBCDIC German	2030
IBM280	IBM EBCDIC Italian	2035
IBM285	IBM EBCDIC UK English	2038
IBM297	IBM EBCDIC French	2040
IBM500	IBM EBCDIC International Latin-1	2044
IBM930	IBM EBCDIC Japanese	930
IBM935	IBM EBCDIC Simplified Chinese	935

Name	Description	ID
IBM937	IBM EBCDIC Traditional Chinese	937
IBM939	IBM EBCDIC Japanese CP939	939
ISO-8859-10	ISO 8859-10 Latin 6 (Nordic)	13
ISO-8859-15	ISO 8859-15 Latin 9 (Western European)	201
ISO-8859-2	ISO 8859-2 Eastern European	5
ISO-8859-3	ISO 8859-3 Southeast European	6
ISO-8859-4	ISO 8859-4 Baltic	7
ISO-8859-5	ISO 8859-5 Cyrillic	8
ISO-8859-6	ISO 8859-6 Arabic	9
ISO-8859-7	ISO 8859-7 Greek	10
ISO-8859-8	ISO 8859-8 Hebrew	11
ISO-8859-9	ISO 8859-9 Latin 5 (Turkish)	12
JapanEUC	Japanese Extended UNIX Code (including JIS X 0212)	18
Latin1	ISO 8859-1 Western European	4
MS1250	MS Windows Latin 2 (Central Europe)	2250
MS1251	MS Windows Cyrillic (Slavic)	2251
MS1252	MS Windows Latin 1 (ANSI), superset of Latin1	2252
MS1253	MS Windows Greek	2253
MS1254	MS Windows Latin 5 (Turkish), superset of ISO 8859-9	2254
MS1255	MS Windows Hebrew	2255
MS1256	MS Windows Arabic	2256
MS1257	MS Windows Baltic Rim	2257
MS1258	MS Windows Vietnamese	2258
MS1361	MS Windows Korean (Johab)	1361
MS874	MS-DOS Thai, superset of TIS 620	874
MS932	MS Windows Japanese, Shift-JIS	2024
MS936	MS Windows Simplified Chinese, superset of GB 2312-80, EUC encoding	936

Name	Description	ID
MS949	MS Windows Korean, superset of KS C 5601-1992	949
MS950	MS Windows Traditional Chinese, superset of Big 5	950
US-ASCII	7-bit ASCII	1
UTF-8	UTF-8 encoding of Unicode	106

Supported Code Pages for Sources and Targets

Informatica supports code pages for internationalization. Informatica uses International Components for Unicode (ICU) for its globalization support. For a list of code page aliases in ICU, see <http://demo.icu-project.org/icu-bin/convexp>.

When you assign a source or target code page in the PowerCenter Client, you select the code page description. When you assign a code page using the *pmrep* CreateConnection command or define a code page in a parameter file, you enter the code page name. The following table lists the name, description, and ID for supported code pages for sources and targets:

Name	Description	ID
Adobe-Standard-Encoding	Adobe Standard Encoding	10073
BOCU-1	Binary Ordered Compression for Unicode (BOCU-1)	10010
CESU-8	ICompatibility Encoding Scheme for UTF-16 (CESU-8)	10011
cp1006	ISO Urdu	10075
cp1098	PC Farsi	10076
cp1124	ISO Cyrillic Ukraine	10077
cp1125	PC Cyrillic Ukraine	10078
cp1131	PC Cyrillic Belarus	10080
cp1381	PC Chinese GB (S-Ch Data mixed)	10082
cp850	PC Latin1	10036
cp851	PC DOS Greek (without euro)	10037
cp856	PC Hebrew (old)	10040
cp857	PC Latin5 (without euro update)	10041
cp858	PC Latin1 (with euro update)	10042

Name	Description	ID
cp860	PC Portugal	10043
cp861	PC Iceland	10044
cp862	PC Hebrew (without euro update)	10045
cp863	PC Canadian French	10046
cp864	PC Arabic (without euro update)	10047
cp865	PC Nordic	10048
cp866	PC Russian (without euro update)	10049
cp868	PC Urdu	10051
cp869	PC Greek (without euro update)	10052
cp922	IPC Estonian (without euro update)	10056
cp949c	PC Korea - KS	10028
ebcdic-xml-us	EBCDIC US (with euro) - Extension for XML4C(Xerces)	10180
EUC-KR	EUC Korean	10029
GB_2312-80	Simplified Chinese (GB2312-80)	10025
gb18030	GB 18030 MBCS codepage	1392
GB2312	Chinese EUC	10024
HKSCS	Hong Kong Supplementary Character Set	9200
hp-roman8	HP Latin1	10072
HZ-GB-2312	Simplified Chinese (HZ GB2312)	10092
IBM037	IBM EBCDIC US English	2028
IBM-1025	EBCDIC Cyrillic	10127
IBM1026	EBCDIC Turkey	10128
IBM1047	IBM EBCDIC US English IBM1047	1047
IBM-1047-s390	EBCDIC IBM-1047 for S/390 (If and nl swapped)	10167
IBM-1097	EBCDIC Farsi	10129
IBM-1112	EBCDIC Baltic	10130
IBM-1122	EBCDIC Estonia	10131

Name	Description	ID
IBM-1123	EBCDIC Cyrillic Ukraine	10132
IBM-1129	ISO Vietnamese	10079
IBM-1130	EBCDIC Vietnamese	10133
IBM-1132	EBCDIC Lao	10134
IBM-1133	ISO Lao	10081
IBM-1137	EBCDIC Devanagari	10163
IBM-1140	EBCDIC US (with euro update)	10135
IBM-1140-s390	EBCDIC IBM-1140 for S/390 (If and nl swapped)	10168
IBM-1141	EBCDIC Germany, Austria (with euro update)	10136
IBM-1142	EBCDIC Denmark, Norway (with euro update)	10137
IBM-1142-s390	EBCDIC IBM-1142 for S/390 (If and nl swapped)	10169
IBM-1143	EBCDIC Finland, Sweden (with euro update)	10138
IBM-1143-s390	EBCDIC IBM-1143 for S/390 (If and nl swapped)	10170
IBM-1144	EBCDIC Italy (with euro update)	10139
IBM-1144-s390	EBCDIC IBM-1144 for S/390 (If and nl swapped)	10171
IBM-1145	EBCDIC Spain, Latin America (with euro update)	10140
IBM-1145-s390	EBCDIC IBM-1145 for S/390 (If and nl swapped)	10172
IBM-1146	EBCDIC UK, Ireland (with euro update)	10141
IBM-1146-s390	EBCDIC IBM-1146 for S/390 (If and nl swapped)	10173
IBM-1147	EBCDIC French (with euro update)	10142
IBM-1147-s390	EBCDIC IBM-1147 for S/390 (If and nl swapped)	10174
IBM-1147-s390	EBCDIC IBM-1147 for S/390 (If and nl swapped)	10174
IBM-1148	EBCDIC International Latin1 (with euro update)	10143
IBM-1148-s390	EBCDIC IBM-1148 for S/390 (If and nl swapped)	10175
IBM-1149	EBCDIC Iceland (with euro update)	10144
IBM-1149-s390	IEBCDIC IBM-1149 for S/390 (If and nl swapped)	10176
IBM-1153	EBCDIC Latin2 (with euro update)	10145

Name	Description	ID
IBM-1153-s390	EBCDIC IBM-1153 for S/390 (lf and nl swapped)	10177
IBM-1154	EBCDIC Cyrillic Multilingual (with euro update)	10146
IBM-1155	EBCDIC Turkey (with euro update)	10147
IBM-1156	EBCDIC Baltic Multilingual (with euro update)	10148
IBM-1157	EBCDIC Estonia (with euro update)	10149
IBM-1158	EBCDIC Cyrillic Ukraine (with euro update)	10150
IBM1159	IBM EBCDIC Taiwan, Traditional Chinese	11001
IBM-1160	EBCDIC Thai (with euro update)	10151
IBM-1162	Thai (with euro update)	10033
IBM-1164	EBCDIC Vietnamese (with euro update)	10152
IBM-1250	MS Windows Latin2 (without euro update)	10058
IBM-1251	MS Windows Cyrillic (without euro update)	10059
IBM-1255	MS Windows Hebrew (without euro update)	10060
IBM-1256	MS Windows Arabic (without euro update)	10062
IBM-1257	MS Windows Baltic (without euro update)	10064
IBM-1258	MS Windows Vietnamese (without euro update)	10066
IBM-12712	EBCDIC Hebrew (updated with euro and new sheqel, control characters)	10161
IBM-12712-s390	EBCDIC IBM-12712 for S/390 (lf and nl swapped)	10178
IBM-1277	Adobe Latin1 Encoding	10074
IBM13121	IBM EBCDIC Korean Extended CP13121	11002
IBM13124	IBM EBCDIC Simplified Chinese CP13124	11003
IBM-1363	PC Korean KSC MBCS Extended (with \ <-> Won mapping)	10032
IBM-1364	EBCDIC Korean Extended (SBCS IBM-13121 combined with DBCS IBM-4930)	10153
IBM-1371	EBCDIC Taiwan Extended (SBCS IBM-1159 combined with DBCS IBM-9027)	10154
IBM-1373	Taiwan Big-5 (with euro update)	10019

Name	Description	ID
IBM-1375	MS Taiwan Big-5 with HKSCS extensions	10022
IBM-1386	PC Chinese GBK (IBM-1386)	10023
IBM-1388	EBCDIC Chinese GB (S-Ch DBCS-Host Data)	10155
IBM-1390	EBCDIC Japanese Katakana (with euro)	10156
IBM-1399	EBCDIC Japanese Latin-Kanji (with euro)	10157
IBM-16684	EBCDIC Japanese Extended (DBCS IBM-1390 combined with DBCS IBM-1399)	10158
IBM-16804	EBCDIC Arabic (with euro update)	10162
IBM-16804-s390	EBCDIC IBM-16804 for S/390 (If and nl swapped)	10179
IBM-25546	ISO-2022 encoding for Korean (extension 1)	10089
IBM273	IBM EBCDIC German	2030
IBM277	EBCDIC Denmark, Norway	10115
IBM278	EBCDIC Finland, Sweden	10116
IBM280	IBM EBCDIC Italian	2035
IBM284	EBCDIC Spain, Latin America	10117
IBM285	IBM EBCDIC UK English	2038
IBM290	EBCDIC Japanese Katakana SBCS	10118
IBM297	IBM EBCDIC French	2040
IBM-33722	Japanese EUC (with \ <-> Yen mapping)	10017
IBM367	IBM367	10012
IBM-37-s390	EBCDIC IBM-37 for S/390 (If and nl swapped)	10166
IBM420	EBCDIC Arabic	10119
IBM424	EBCDIC Hebrew (updated with new sheqel, control characters)	10120
IBM437	PC United States	10035
IBM-4899	EBCDIC Hebrew (with euro)	10159
IBM-4909	ISO Greek (with euro update)	10057
IBM4933	IBM Simplified Chinese CP4933	11004

Name	Description	ID
IBM-4971	EBCDIC Greek (with euro update)	10160
IBM500	IBM EBCDIC International Latin-1	2044
IBM-5050	Japanese EUC (Packed Format)	10018
IBM-5123	EBCDIC Japanese Latin (with euro update)	10164
IBM-5351	MS Windows Hebrew (older version)	10061
IBM-5352	MS Windows Arabic (older version)	10063
IBM-5353	MS Windows Baltic (older version)	10065
IBM-803	EBCDIC Hebrew	10121
IBM833	IBM EBCDIC Korean CP833	833
IBM834	IBM EBCDIC Korean CP834	834
IBM835	IBM Taiwan, Traditional Chinese CP835	11005
IBM836	IBM EBCDIC Simplified Chinese Extended	11006
IBM837	IBM Simplified Chinese CP837	11007
IBM-838	EBCDIC Thai	10122
IBM-8482	EBCDIC Japanese Katakana SBCS (with euro update)	10165
IBM852	PC Latin2 (without euro update)	10038
IBM855	PC Cyrillic (without euro update)	10039
IBM-867	PC Hebrew (with euro update)	10050
IBM870	EBCDIC Latin2	10123
IBM871	EBCDIC Iceland	10124
IBM-874	PC Thai (without euro update)	10034
IBM-875	EBCDIC Greek	10125
IBM-901	PC Baltic (with euro update)	10054
IBM-902	PC Estonian (with euro update)	10055
IBM918	EBCDIC Urdu	10126
IBM930	IBM EBCDIC Japanese	930
IBM933	IBM EBCDIC Korean CP933	933

Name	Description	ID
IBM935	IBM EBCDIC Simplified Chinese	935
IBM937	IBM EBCDIC Traditional Chinese	937
IBM939	IBM EBCDIC Japanese CP939	939
IBM-942	PC Japanese SJIS-78 syntax (IBM-942)	10015
IBM-943	PC Japanese SJIS-90 (IBM-943)	10016
IBM-949	PC Korea - KS (default)	10027
IBM-950	Taiwan Big-5 (without euro update)	10020
IBM-964	EUC Taiwan	10026
IBM-971	EUC Korean (DBCS-only)	10030
IMAP-mailbox-name	IMAP Mailbox Name	10008
is-960	Israeli Standard 960 (7-bit Hebrew encoding)	11000
ISO-2022-CN	ISO-2022 encoding for Chinese	10090
ISO-2022-CN-EXT	ISO-2022 encoding for Chinese (extension 1)	10091
ISO-2022-JP	ISO-2022 encoding for Japanese	10083
ISO-2022-JP-2	ISO-2022 encoding for Japanese (extension 2)	10085
ISO-2022-KR	ISO-2022 encoding for Korean	10088
ISO-8859-10	ISO 8859-10 Latin 6 (Nordic)	13
ISO-8859-13	ISO 8859-13 PC Baltic (without euro update)	10014
ISO-8859-15	ISO 8859-15 Latin 9 (Western European)	201
ISO-8859-2	ISO 8859-2 Eastern European	5
ISO-8859-3	ISO 8859-3 Southeast European	6
ISO-8859-4	ISO 8859-4 Baltic	7
ISO-8859-5	ISO 8859-5 Cyrillic	8
ISO-8859-6	ISO 8859-6 Arabic	9
ISO-8859-7	ISO 8859-7 Greek	10
ISO-8859-8	ISO 8859-8 Hebrew	11
ISO-8859-9	ISO 8859-9 Latin 5 (Turkish)	12

Name	Description	ID
JapanEUC	Japanese Extended UNIX Code (including JIS X 0212)	18
JEF	Japanese EBCDIC Fujitsu	9000
JEF-K	Japanese EBCDIC-Kana Fujitsu	9005
JIPSE	NEC ACOS JIPSE Japanese	9002
JIPSE-K	NEC ACOS JIPSE-Kana Japanese	9007
JIS_Encoding	ISO-2022 encoding for Japanese (extension 1)	10084
JIS_X0201	ISO-2022 encoding for Japanese (JIS_X0201)	10093
JIS7	ISO-2022 encoding for Japanese (extension 3)	10086
JIS8	ISO-2022 encoding for Japanese (extension 4)	10087
JP-EBCDIC	EBCDIC Japanese	9010
JP-EBCDIK	EBCDIK Japanese	9011
KEIS	HITACHI KEIS Japanese	9001
KEIS-K	HITACHI KEIS-Kana Japanese	9006
KOI8-R	IRussian Internet	10053
KSC_5601	PC Korean KSC MBCS Extended (KSC_5601)	10031
Latin1	ISO 8859-1 Western European	4
LMBCS-1	Lotus MBCS encoding for PC Latin1	10103
LMBCS-11	Lotus MBCS encoding for MS-DOS Thai	10110
LMBCS-16	Lotus MBCS encoding for Windows Japanese	10111
LMBCS-17	Lotus MBCS encoding for Windows Korean	10112
LMBCS-18	Lotus MBCS encoding for Windows Chinese (Traditional)	10113
LMBCS-19	Lotus MBCS encoding for Windows Chinese (Simplified)	10114
LMBCS-2	Lotus MBCS encoding for PC DOS Greek	10104
LMBCS-3	Lotus MBCS encoding for Windows Hebrew	10105
LMBCS-4	Lotus MBCS encoding for Windows Arabic	10106
LMBCS-5	Lotus MBCS encoding for Windows Cyrillic	10107
LMBCS-6	Lotus MBCS encoding for PC Latin2	10108

Name	Description	ID
LMBCS-8	Lotus MBCS encoding for Windows Turkish	10109
macintosh	Apple Latin 1	10067
MELCOM	MITSUBISHI MELCOM Japanese	9004
MELCOM-K	MITSUBISHI MELCOM-Kana Japanese	9009
MS1250	MS Windows Latin 2 (Central Europe)	2250
MS1251	MS Windows Cyrillic (Slavic)	2251
MS1252	MS Windows Latin 1 (ANSI), superset of Latin1	2252
MS1253	MS Windows Greek	2253
MS1254	MS Windows Latin 5 (Turkish), superset of ISO 8859-9	2254
MS1255	MS Windows Hebrew	2255
MS1256	MS Windows Arabic	2256
MS1257	MS Windows Baltic Rim	2257
MS1258	MS Windows Vietnamese	2258
MS1361	MS Windows Korean (Johab)	1361
MS874	MS-DOS Thai, superset of TIS 620	874
MS932	MS Windows Japanese, Shift-JIS	2024
MS936	MS Windows Simplified Chinese, superset of GB 2312-80, EUC encoding	936
MS949	MS Windows Korean, superset of KS C 5601-1992	949
MS950	MS Windows Traditional Chinese, superset of Big 5	950
SCSU	Standard Compression Scheme for Unicode (SCSU)	10009
UNISYS	UNISYS Japanese	9003
UNISYS-K	UNISYS-Kana Japanese	9008
US-ASCII	7-bit ASCII	1
UTF-16_OppositeEndian	UTF-16 encoding of Unicode (Opposite Platform Endian)	10004
UTF-16_PlatformEndian	UTF-16 encoding of Unicode (Platform Endian)	10003
UTF-16BE	UTF-16 encoding of Unicode (Big Endian)	1200

Name	Description	ID
UTF-16LE	UTF-16 encoding of Unicode (Lower Endian)	1201
UTF-32_OppositeEndian	UTF-32 encoding of Unicode (Opposite Platform Endian)	10006
UTF-32_PlatformEndian	UTF-32 encoding of Unicode (Platform Endian)	10005
UTF-32BE	UTF-32 encoding of Unicode (Big Endian)	10001
UTF-32LE	UTF-32 encoding of Unicode (Lower Endian)	10002
UTF-7	UTF-7 encoding of Unicode	10007
UTF-8	UTF-8 encoding of Unicode	106
windows-57002	Indian Script Code for Information Interchange - Devanagari	10094
windows-57003	Indian Script Code for Information Interchange - Bengali	10095
windows-57004	Indian Script Code for Information Interchange - Tamil	10099
windows-57005	Indian Script Code for Information Interchange - Telugu	10100
windows-57007	Indian Script Code for Information Interchange - Oriya	10098
windows-57008	Indian Script Code for Information Interchange - Kannada	10101
windows-57009	Indian Script Code for Information Interchange - Malayalam	10102
windows-57010	Indian Script Code for Information Interchange - Gujarati	10097
windows-57011	Indian Script Code for Information Interchange - Gurmukhi	10096
x-mac-centraleurroman	Apple Central Europe	10070
x-mac-cyrillic	Apple Cyrillic	10069
x-mac-greek	Apple Greek	10068
x-mac-turkish	Apple Turkish	10071

Restrictions for Code Pages for Sources and Targets

Consider the following restrictions when you assign a source or target code page:

- Select IBM EBCDIC as your source database connection code page only if you access EBCDIC data, such as data from a mainframe extract file.
- The following code pages are not supported for database or relational connections:
 - UTF-16 encoding of Unicode (Opposite Platform Endian)
 - UTF-16 encoding of Unicode (Platform Endian)
 - UTF-16 encoding of Unicode (Big Endian)
 - UTF-16 encoding of Unicode (Lower Endian)

APPENDIX B

Command Line Privileges and Permissions

This appendix includes the following topics:

- [infacmd as Commands, 257](#)
- [infacmd dis Commands, 258](#)
- [infacmd ipc Commands, 259](#)
- [infacmd isp Commands, 260](#)
- [infacmd mrs Commands, 271](#)
- [infacmd ms Commands, 272](#)
- [infacmd oie Commands, 272](#)
- [infacmd ps Commands, 272](#)
- [infacmd pwx Commands, 273](#)
- [infacmd rtm Commands, 274](#)
- [infacmd sql Commands, 275](#)
- [infacmd rds Commands, 276](#)
- [infacmd wfs Commands, 276](#)
- [pmcmd Commands, 276](#)
- [pmrep Commands, 278](#)

infacmd as Commands

To run *infacmd as* commands, users must have one of the listed sets of domain privileges, Analyst Service privileges, and domain object permissions.

The following table lists the required privileges and permissions for *infacmd* as commands:

infacmd as Command	Privilege Group	Privilege Name	Permission On...
CreateAuditTables	Domain Administration	Manage Service	Domain or node where Analyst Service runs
CreateService	Domain Administration	Manage Service	Domain or node where Analyst Service runs
DeleteAuditTables	Domain Administration	Manage Service	Domain or node where Analyst Service runs
ListServiceOptions	-	-	Analyst Service
ListServiceProcessOptions	-	-	Analyst Service
UpdateServiceOptions	Domain Administration	Manage Service	Domain or node where Analyst Service runs
UpdateServiceProcessOptions	Domain Administration	Manage Service	Domain or node where Analyst Service runs

infacmd dis Commands

To run *infacmd dis* commands, users must have one of the listed sets of domain privileges, Data Integration Service privileges, and domain object permissions.

The following table lists the required privileges and permissions for *infacmd dis* commands:

infacmd dis Command	Privilege Group	Privilege Name	Permission On...
BackupApplication	Application Administration	Manage Applications	-
CancelDataObjectCache Refresh	-	-	-
CreateService	Domain Administration	Manage Services	Domain or node where Data Integration Service runs
DeployApplication	Application Administration	Manage Applications	-
ListApplicationObjects	-	-	-
ListApplications	-	-	-

infacmd dis Command	Privilege Group	Privilege Name	Permission On...
ListDataObjectOptions	-	-	-
ListServiceOptions	-	Manage Service	Domain or node where Data Integration Service runs
ListServiceProcessOptions	-	Manage Service	Domain or node where Data Integration Service runs
PurgeDataObjectCache	-	-	-
RefreshDataObjectCache	-	-	-
RenameApplication	Application Administration	Manage Applications	-
RestoreApplication	Application Administration	Manage Applications	-
StartApplication	Application Administration	Manage Applications	-
StopApplication	Application Administration	Manage Applications	-
UndeployApplication	Application Administration	Manage Applications	-
UpdateApplication	Application Administration	Manage Applications	-
UpdateApplicationOptions	Application Administration	Manage Applications	-
UpdateDataObjectOptions	Application Administration	Manage Applications	-
UpdateServiceOptions	Domain Administration	Manage Services	Domain or node where Data Integration Service runs
UpdateServiceProcessOptions	Domain Administration	Manage Services	Domain or node where Data Integration Service runs

infacmd ipc Commands

To run *infacmd ipc* commands, users must have one of the listed Model repository object permissions.

The following table lists the required privileges and permissions for *infacmd ipc* commands:

infacmd ipc Command	Privilege Group	Privilege Name	Permission On...
ExportToPC	-	-	Read on the folder that creates reference tables to be exported

infacmd isp Commands

To run *infacmd isp* commands, users must have one of the listed sets of domain privileges, service privileges, domain object permissions, and connection permissions.

Users must be assigned the Administrator role for the domain to run the following commands:

- AddDomainLink
- AssignGroupPermission (on domain)
- AssignGroupPermission (on operating system profiles)
- AddServiceLevel
- AssignUserPermission (on domain)
- AssignUserPermission (on operating system profiles)
- CreateOSProfile
- PurgeLog
- RemoveDomainLink
- RemoveOSProfile
- RemoveServiceLevel
- SwitchToGatewayNode
- SwitchToWorkerNode
- UpdateDomainOptions
- UpdateDomainPassword
- UpdateGatewayInfo
- UpdateServiceLevel
- UpdateSMTPOptions

Users must be assigned the Administrator role for the domain to run the UpdateGatewayInfo command.

The following table lists the required privileges and permissions for *infacmd isp* commands:

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
AddAlertUser (for your user account)	-	-	-
AddAlertUser (for other users)	Security Administration	Manage Users, Groups, and Roles	-

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
AddConnectionPermissions	-	-	Grant on connection
AddDomainLink	-	-	-
AddDomainNode	Domain Administration	Manage Nodes and Grids	Domain and node
AssignGroupPermission (on application services or license objects)	Domain Administration	Manage Services	Application service or license object
AssignGroupPermission (on domain)	-	-	-
AssignGroupPermission (on folders)	Domain Administration	Manage Domain Folders	Folder
AssignGroupPermission (on nodes and grids)	Domain Administration	Manage Nodes and Grids	Node or grid
AssignGroupPermission (on operating system profiles)	-	-	-
AddGroupPrivilege	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
AddLicense	Domain Administration	Manage Services	Domain or parent folder
AddNodeResource	Domain Administration	Manage Nodes and Grids	Node
AddRolePrivilege	Security Administration	Manage Users, Groups, and Roles	-
AddServiceLevel	-	-	-
AssignUserPermission (on application services or license objects)	Domain Administration	Manage Services	Application service or license object
AssignUserPermission (on domain)	-	-	-
AssignUserPermission (on folders)	Domain Administration	Manage Domain Folders	Folder
AssignUserPermission (on nodes or grids)	Domain Administration	Manage Nodes and Grids	Node or grid
AssignUserPermission (on operating system profiles)	-	-	-

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
AssignUserPrivilege	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
AssignUserToGroup	Security Administration	Manage Users, Groups, and Roles	-
AssignedToLicense	Domain Administration	Manage Services	License object and application service
AssignISTOMMService	Domain Administration	Manage Services	Metadata Manager Service
AssignLicense	Domain Administration	Manage Services	License object and application service
AssignRoleToGroup	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
AssignRoleToUser	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
AssignRSToWSHubService	Domain Administration	Manage Services	PowerCenter Repository Service and Web Services Hub
BackupReportingServiceContents	Domain Administration	Manage Services	Reporting Service
ConvertLogFile	-	-	Domain or application service
CreateFolder	Domain Administration	Manage Domain Folders	Domain or parent folder
CreateConnection	-	-	-
CreateGrid	Domain Administration	Manage Nodes and Grids	Domain or parent folder and nodes assigned to grid

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
CreateGroup	Security Administration	Manage Users, Groups, and Roles	-
CreateIntegrationService	Domain Administration	Manage Services	Domain or parent folder, node or grid where PowerCenter Integration Service runs, license object, and associated PowerCenter Repository Service
CreateMMService	Domain Administration	Manage Services	Domain or parent folder, node where Metadata Manager Service runs, license object, and associated PowerCenter Integration Service and PowerCenter Repository Service
CreateOSProfile	-	-	-
CreateReportingService	Domain Administration	Manage Services	Domain or parent folder, node where Reporting Service runs, license object, and the application service selected for reporting
CreateReportingServiceContents	Domain Administration	Manage Services	Reporting Service
CreateRepositoryService	Domain Administration	Manage Services	Domain or parent folder, node where PowerCenter Repository Service runs, and license object
CreateRole	Security Administration	Manage Users, Groups, and Roles	-
CreateSAPBWService	Domain Administration	Manage Services	Domain or parent folder, node or grid where SAP BW Service runs, license object, and associated PowerCenter Integration Service

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
CreateUser	Security Administration	Manage Users, Groups, and Roles	-
CreateWSHubService	Domain Administration	Manage Services	Domain or parent folder, node or grid where Web Services Hub runs, license object, and associated PowerCenter Repository Service
DeleteSchemaReportingServiceContents	Domain Administration	Manage Services	Reporting Service
DisableNodeResource	Domain Administration	Manage Nodes and Grids	Node
DisableService (for Metadata Manager Service)	Domain Administration	Manage Service Execution	Metadata Manager Service and associated PowerCenter Integration Service and PowerCenter Repository Service
DisableService (for all other application services)	Domain Administration	Manage Service Execution	Application service
DisableServiceProcess	Domain Administration	Manage Service Execution	Application service
DisableUser	Security Administration	Manage Users, Groups, and Roles	-
EditUser	Security Administration	Manage Users, Groups, and Roles	-
EnableNodeResource	Domain Administration	Manage Nodes and Grids	Node
EnableService (for Metadata Manager Service)	Domain Administration	Manage Service Execution	Metadata Manager Service, and associated PowerCenter Integration Service and PowerCenter Repository Service
EnableService (for all other application services)	Domain Administration	Manage Service Execution	Application service
EnableServiceProcess	Domain Administration	Manage Service Execution	Application service

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
EnableUser	Security Administration	Manage Users, Groups, and Roles	-
ExportDomainObjects (for users, groups, and roles)	Security Administration	Manage Users, Groups, and Roles	-
ExportDomainObjects (for connections)	Domain Administration	Manage Connections	Read on connections
ExportUsersAndGroups	Security Administration	Manage Users, Groups, and Roles	-
GetFolderInfo	-	-	Folder
GetLastError	-	-	Application service
GetLog	-	-	Domain or application service
GetNodeName	-	-	Node
GetServiceOption	-	-	Application service
GetServiceProcessOption	-	-	Application service
GetServiceProcessStatus	-	-	Application service
GetServiceStatus	-	-	Application service
GetSessionLog	Run-time Objects	Monitor	Read on repository folder
GetWorkflowLog	Run-time Objects	Monitor	Read on repository folder
Help	-	-	-
ImportDomainObjects (for users, groups, and roles)	Security Administration	Manage Users, Groups, and Roles	-
ImportDomainObjects (for connections)	Domain Administration	Manage Connections	Write on connections
ImportUsersAndGroups	Security Administration	Manage Users, Groups, and Roles	-
ListAlertUsers	-	-	Domain
ListAllGroups	-	-	-

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
ListAllRoles	-	-	-
ListAllUsers	-	-	-
ListConnectionOptions	-	-	Read on connection
ListConnections	-	-	-
ListConnectionPermissions	-	-	-
ListConnectionPermissions by Group	-	-	-
ListConnectionPermissions by User	-	-	-
ListDomainLinks	-	-	Domain
ListDomainOptions	-	-	Domain
ListFolders	-	-	Folders
ListGridNodes	-	-	-
ListGroupsForUser	-	-	Domain
ListGroupPermissions	-	-	-
ListGroupPrivilege	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
ListLDAPConnectivity	Security Administration	Manage Users, Groups, and Roles	-
ListLicenses	-	-	License objects
ListNodeOptions	-	-	Node
ListNodes	-	-	-
ListNodeResources	-	-	Node
ListPlugins	-	-	-
ListRepositoryLDAPConfiguration	-	-	Domain
ListRolePrivileges	-	-	-
ListSecurityDomains	Security Administration	Manage Users, Groups, and Roles	-

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
ListServiceLevels	-	-	Domain
ListServiceNodes	-	-	Application service
ListServicePrivileges	-	-	-
ListServices	-	-	-
ListSMTPOptions	-	-	Domain
ListUserPermissions	-	-	-
ListUserPrivilege	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
MigrateReportingServiceContents	Domain Administration and Security Administration	Manage Services and Manage Users, Groups, and Roles	Domain
MoveFolder	Domain Administration	Manage Domain Folders	Original and destination folders
MoveObject (for application services or license objects)	Domain Administration	Manage Services	Original and destination folders
MoveObject (for nodes or grids)	Domain Administration	Manage Nodes and Grids	Original and destination folders
Ping	-	-	-
PurgeLog	-	-	-
RemoveAlertUser (for your user account)	-	-	-
RemoveAlertUser (for other users)	Security Administration	Manage Users, Groups, and Roles	-
RemoveConnection	-	-	Write on connection
RemoveConnectionPermissions	-	-	Grant on connection
RemoveDomainLink	-	-	-
RemoveFolder	Domain Administration	Manage Domain Folders	Domain or parent folder and folder being removed
RemoveGrid	Domain Administration	Manage Nodes and Grids	Domain or parent folder and grid

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
RemoveGroup	Security Administration	Manage Users, Groups, and Roles	-
RemoveGroupPrivilege	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
RemoveLicense	Domain Administration	Manage Services	Domain or parent folder and license object
RemoveNode	Domain Administration	Manage Nodes and Grids	Domain or parent folder and node
RemoveNodeResource	Domain Administration	Manage Nodes and Grids	Node
RemoveOSProfile	-	-	-
RemoveRole	Security Administration	Manage Users, Groups, and Roles	-
RemoveRolePrivilege	Security Administration	Manage Users, Groups, and Roles	-
RemoveService	Domain Administration	Manage Services	Domain or parent folder and application service
RemoveServiceLevel	-	-	-
RemoveUser	Security Administration	Manage Users, Groups, and Roles	-
RemoveUserFromGroup	Security Administration	Manage Users, Groups, and Roles	-
RemoveUserPrivilege	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
RenameConnection	-	-	Write on connection
ResetPassword (for your user account)	-	-	-

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
ResetPassword (for other users)	Security Administration	Manage Users, Groups, and Roles	-
RestoreReportingServiceContents	Domain Administration	Manage Services	Reporting Service
RunCPUProfile	Domain Administration	Manage Nodes and Grids	Node
SetConnectionPermission	-	-	Grant on connection
SetLDAPConnectivity	Security Administration	Manage Users, Groups, and Roles	-
SetRepositoryLDAPConfiguration	-	-	Domain
ShowLicense	-	-	License object
ShutdownNode	Domain Administration	Manage Nodes and Grids	Node
SwitchToGatewayNode	-	-	-
SwitchToWorkerNode	-	-	-
UnAssignISMMService	Domain Administration	Manage Services	PowerCenter Integration Service and Metadata Manager Service
UnassignLicense	Domain Administration	Manage Services	License object and application service
UnAssignRoleFromGroup	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
UnAssignRoleFromUser	Security Administration	Grant Privileges and Roles	Domain, Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, or Reporting Service
UnassignRSWSHubService	Domain Administration	Manage Services	PowerCenter Repository Service and Web Services Hub
UnassociateDomainNode	Domain Administration	Manage Nodes and Grids	Node

infacmd isp Command	Privilege Group	Privilege Name	Permission On...
UpdateConnection	-	-	Write on connection
UpdateDomainOptions	-	-	-
UpdateDomainPassword	-	-	-
UpdateFolder	Domain Administration	Manage Domain Folders	Folder
UpdateGatewayInfo	-	-	-
UpdateGrid	Domain Administration	Manage Nodes and Grids	Grid and nodes
UpdateIntegrationService	Domain Administration	Manage Services	PowerCenter Integration Service
UpdateLicense	Domain Administration	Manage Services	License object
UpdateMMService	Domain Administration	Manage Services	Metadata Manager Service
UpdateNodeOptions	Domain Administration	Manage Nodes and Grids	Node
UpdateOSProfile	Security Administration	Manage Users, Groups, and Roles	Operating system profile
UpdateReportingService	Domain Administration	Manage Services	Reporting Service
UpdateRepositoryService	Domain Administration	Manage Services	PowerCenter Repository Service
UpdateSAPBWService	Domain Administration	Manage Services	SAP BW Service
UpdateServiceLevel	-	-	-
UpdateServiceProcess	Domain Administration	Manage Services	PowerCenter Integration Service Each node added to the PowerCenter Integration Service
UpdateSMTPOptions	-	-	-
UpdateWSHubService	Domain Administration	Manage Services	Web Services Hub
UpgradeReportingServiceContents	Domain Administration	Manage Services	Reporting Service

infacmd mrs Commands

To run *infacmd mrs* commands, users must have one of the listed sets of domain privileges, Model Repository Service privileges, and Model repository object permissions.

The following table lists the required privileges and permissions for *infacmd mrs* commands:

infacmd mrs Command	Privilege Group	Privilege Name	Permission On...
BackupContents	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
CreateContents	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
CreateService	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
DeleteContents	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
ListBackupFiles	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
ListProjects	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
ListServiceOptions	-	-	The Model Repository Service
ListServiceProcessOptions	-	-	The Model Repository Service
RestoreContents	Domain Administration	Manage Service	Domain or node where the Model Repository Service runs
UpgradeContents	Model Repository Service Administration	Create, Edit and Delete Projects	Write on projects
UpdateServiceOptions	Domain Administration	Manage Service	The Model Repository Service
UpdateServiceProcessOptions	Domain Administration	Manage Service	The Model Repository Service

infacmd ms Commands

To run *infacmd ms* commands, users must have one of the listed sets of domain object permissions.

The following table lists the required privileges and permissions for *infacmd ms* commands:

infacmd ms Command	Privilege Group	Privilege Name	Permission On...
ListMappings	-	-	-
ListMappingParams	-	-	-
RunMapping	-	-	Execute on connection objects used by the mapping

infacmd oie Commands

To run *infacmd oie* commands, users must have one of the listed Model repository object permissions.

The following table lists the required permissions for *infacmd oie* commands:

infacmd oie Command	Privilege Group	Privilege Name	Permission On...
ExportObjects	-	-	Read on project
ImportObjects	-	-	Write on project

infacmd ps Commands

To run *infacmd ps* commands, users must have one of the listed sets of profiling privileges and domain object permissions.

The following table lists the required privileges and permissions for *infacmd ps* commands:

infacmd ps Command	Privilege Group	Privilege Name	Permission On...
CreateWH	-	-	-
DropWH	-	-	-
Execute	-	-	Read on project Execute on the source connection object

infacmd ps Command	Privilege Group	Privilege Name	Permission On...
List	-	-	Read on project
Purge	-	-	Read and write on project

infacmd pwx Commands

To run *infacmd pwx* commands, users must have one of the listed sets of PowerExchange application service permissions and privileges.

The following table lists the required privileges and permissions for *infacmd pwx* commands:

infacmd pwx Command	Privilege Group	Privilege Name	Permission On...
CloseForceListener	Management Commands	closeforce	-
CloseListener	Management Commands	close	-
CondenseLogger	Management Commands	condense	-
CreateListenerService	Domain Administration	Manage Service	Domain or node where the PowerExchange application service runs
CreateLoggerService	Domain Administration	Manage Service	Domain or node where the PowerExchange application service runs
DisplayAllLogger	Informational Commands	displayall	-
DisplayCheckpointsLogger	Informational Commands	displaycheckpoints	-
DisplayCPULogger	Informational Commands	displaycpu	-
DisplayEventsLogger	Informational Commands	displayevents	-
DisplayMemoryLogger	Informational Commands	displaymemory	-

infacmd pwx Command	Privilege Group	Privilege Name	Permission On...
DisplayRecordsLogger	Informational Commands	displayrecords	-
DisplayStatusLogger	Informational Commands	displaystatus	-
FileSwitchLogger	Management Commands	fileswitch	-
ListTaskListener	Informational Commands	listtask	-
ShutDownLogger	Management Commands	shutdown	-
StopTaskListener	Management Commands	stoptask	-
UpdateListenerService	Domain Administration	Manage Service	Domain or node where the PowerExchange application service runs
UpdateLoggerService	Domain Administration	Manage Service	Domain or node where the PowerExchange application service runs

infacmd rtm Commands

To run *infacmd rtm* commands, users must have one of the listed sets of Model Repository Service privileges and domain object permissions.

The following table lists the required privileges and permissions for *infacmd rtm* commands:

infacmd rtm Command	Privilege Group	Privilege Name	Permission On...
Deployimport	-	-	-
Export	-	-	Read on the project that contains reference tables to be exported
Import	-	-	Read and Write on the project where reference tables are imported

infacmd sql Commands

To run *infacmd sql* commands, users must have one of the listed sets of domain privileges, Data Integration Service privileges, and domain object permissions.

The following table lists the required privileges and permissions for *infacmd sql* commands:

infacmd sql Command	Privilege Group	Privilege Name	Permission On...
ExecuteSQL	-	-	Based on objects that you want to access in your SQL statement
ListColumnPermissions	-	-	-
ListSQLDataServiceOptions	-	-	-
ListSQLDataServicePermissions	-	-	-
ListSQLDataServices	-	-	-
ListStoredProcedurePermissions	-	-	-
ListTableOptions	-	-	-
ListTablePermissions	-	-	-
PurgeTableCache	-	-	-
RefreshTableCache	-	-	-
RenameSQLDataService	Application Administration	Manage Applications	-
SetColumnPermissions	-	-	Grant on the object
SetSQLDataServicePermissions	-	-	Grant on the object
SetStoredProcedurePermissions	-	-	Grant on the object
SetTablePermissions	-	-	Grant on the object
StartSQLDataService	Application Administration	Manage Applications	-
StopSQLDataService	Application Administration	Manage Applications	-
UpdateColumnOptions	Application Administration	Manage Applications	-
UpdateSQLDataServiceOptions	Application Administration	Manage Applications	-
UpdateTableOptions	Application Administration	Manage Applications	-

infacmd rds Commands

To run `infacmd rds` commands, users must have one of the listed sets of domain privileges, Reporting and Dashboards Service privileges, and domain object permissions.

The following table lists the required privileges and permissions for `infacmd rds` commands:

infacmd rds Command	Privilege Group	Privilege Name	Permission On...
CreateService	Domain Administration	Manage Service	Domain or node where the Reporting and Dashboards Service runs
ListServiceProcessOptions	-	-	The Reporting and Dashboards Service

infacmd wfs Commands

To run `infacmd wfs` commands, users do not require any privileges or permissions.

pmcmd Commands

To run `pmcmd` commands, users must have the listed sets of PowerCenter Repository Service privileges and PowerCenter repository object permissions.

When the PowerCenter Integration Service runs in safe mode, users must have the Administrator role for the associated PowerCenter Repository Service to run the following commands:

- aborttask
- abortworkflow
- getrunningessionsdetails
- getservicedetails
- getsessionstatistics
- gettaskdetails
- getworkflowdetails
- recoverworkflow
- scheduleworkflow
- starttask
- startworkflow
- stoptask
- stopworkflow
- unscheduleworkflow

The following table lists the required privileges and permissions for *pmcmd* commands:

pmcmd Command	Privilege Group	Privilege Name	Permission
aborttask (started by own user account)	-	-	Read and Execute on folder
aborttask (started by other users)	Run-time Objects	Manage Execution	Read and Execute on folder
abortworkflow (started by own user account)	-	-	Read and Execute on folder
abortworkflow (started by other users)	Run-time Objects	Manage Execution	Read and Execute on folder
connect	-	-	-
disconnect	-	-	-
exit	-	-	-
getrunningessionsdetails	Run-time Objects	Monitor	-
getservicedetails	Run-time Objects	Monitor	Read on folder
getserviceproperties	-	-	-
getsessionstatistics	Run-time Objects	Monitor	Read on folder
gettaskdetails	Run-time Objects	Monitor	Read on folder
getworkflowdetails	Run-time Objects	Monitor	Read on folder
help	-	-	-
pingservice	-	-	-
recoverworkflow (started by own user account)	Run-time Objects	Execute	Read and Execute on folder Read and Execute on connection object Permission on operating system profile (if applicable)
recoverworkflow (started by other users)	Run-time Objects	Manage Execution	Read and Execute on folder Read and Execute on connection object Permission on operating system profile (if applicable)
scheduleworkflow	Run-time Objects	Manage Execution	Read and Execute on folder Read and Execute on connection object Permission on operating system profile (if applicable)

pmcmd Command	Privilege Group	Privilege Name	Permission
setfolder	-	-	Read on folder
setnowait	-	-	-
setwait	-	-	-
showsettings	-	-	-
starttask	Run-time Objects	Execute	Read and Execute on folder Read and Execute on connection object Permission on operating system profile (if applicable)
startworkflow	Run-time Objects	Execute	Read and Execute on folder Read and Execute on connection object Permission on operating system profile (if applicable)
stoptask (started by own user account)	-	-	Read and Execute on folder
stoptask (started by other users)	Run-time Objects	Manage Execution	Read and Execute on folder
stopworkflow (started by own user account)	-	-	Read and Execute on folder
stopworkflow (started by other users)	Run-time Objects	Manage Execution	Read and Execute on folder
unscheduleworkflow	Run-time Objects	Manage Execution	Read and Execute on folder
unsetfolder	-	-	Read on folder
version	-	-	-
waittask	Run-time Objects	Monitor	Read on folder
waitworkflow	Run-time Objects	Monitor	Read on folder

pmrep Commands

Users must have the Access Repository Manager privilege to run all *pmrep* commands except for the following commands:

- Run
- Create
- Restore

- Upgrade
- Version
- Help

To run *pmrep* commands, users must have one of the listed sets of domain privileges, PowerCenter Repository Service privileges, domain object permissions, and PowerCenter repository object permissions.

Users must be the object owner or have the Administrator role for the PowerCenter Repository Service to run the following commands:

- AssignPermission
- ChangeOwner
- DeleteConnection
- DeleteDeploymentGroup
- DeleteFolder
- DeleteLabel
- ModifyFolder (to change owner, configure permissions, designate the folder as shared, or edit the folder name or description)

The following table lists the required privileges and permissions for *pmrep* commands:

pmrep Command	Privilege Group	Privilege Name	Permission
AddToDeploymentGroup	Global Objects	Manage Deployment Groups	Read on original folder Read and Write on deployment group
ApplyLabel	-	-	Read on folder Read and Execute on label
AssignPermission	-	-	-
BackUp	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
ChangeOwner	-	-	-
CheckIn (for your own checkouts)	Design Objects	Create, Edit, and Delete	Read and Write on folder
CheckIn (for your own checkouts)	Sources and Targets	Create, Edit, and Delete	Read and Write on folder
CheckIn (for your own checkouts)	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
CheckIn (for others' checkouts)	Design Objects	Manage Versions	Read and Write on folder
CheckIn (for others' checkouts)	Sources and Targets	Manage Versions	Read and Write on folder
CheckIn (for others' checkouts)	Run-time Objects	Manage Versions	Read and Write on folder

pmrep Command	Privilege Group	Privilege Name	Permission
CleanUp	-	-	-
ClearDeploymentGroup	Global Objects	Manage Deployment Groups	Read and Write on deployment group
Connect	-	-	-
Create	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
CreateConnection	Global Objects	Create Connections	-
CreateDeploymentGroup	Global Objects	Manage Deployment Groups	-
CreateFolder	Folders	Create	-
CreateLabel	Global Objects	Create Labels	-
Delete	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
DeleteConnection	-	-	-
DeleteDeploymentGroup	-	-	-
DeleteFolder	-	-	-
DeleteLabel	-	-	-
DeleteObject	Design Objects	Create, Edit, and Delete	Read and Write on folder
DeleteObject	Sources and Targets	Create, Edit, and Delete	Read and Write on folder
DeleteObject	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
DeployDeploymentGroup	Global Objects	Manage Deployment Groups	Read on original folder Read and Write on destination folder Read and Execute on deployment group
DeployFolder	Folders	Copy on original repository Create on destination repository	Read on folder
ExecuteQuery	-	-	Read and Execute on query
Exit	-	-	-

pmrep Command	Privilege Group	Privilege Name	Permission
FindCheckout	-	-	Read on folder
GetConnectionDetails	-	-	Read on connection object
Help	-	-	-
KillUserConnection	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
ListConnections	-	-	Read on connection object
ListObjectDependencies	-	-	Read on folder
ListObjects	-	-	Read on folder
ListTablesBySess	-	-	Read on folder
ListUserConnections	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
ModifyFolder (to change owner, configure permissions, designate the folder as shared, or edit the folder name or description)	-	-	-
ModifyFolder (to change status)	Folders	Manage Versions	Read and Write on folder
Notify	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
ObjectExport	-	-	Read on folder
ObjectImport	Design Objects	Create, Edit, and Delete	Read and Write on folder
ObjectImport	Sources and Targets	Create, Edit, and Delete	Read and Write on folder
ObjectImport	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
PurgeVersion	Design Objects	Manage Versions	Read and Write on folder Read, Write, and Execute on query if you specify a query name
PurgeVersion	Sources and Targets	Manage Versions	Read and Write on folder Read, Write, and Execute on query if you specify a query name

pmrep Command	Privilege Group	Privilege Name	Permission
PurgeVersion	Run-time Objects	Manage Versions	Read and Write on folder Read, Write, and Execute on query if you specify a query name
PurgeVersion (to purge objects at the folder level)	Folders	Manage Versions	Read and Write on folder
PurgeVersion (to purge objects at the repository level)	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
Register	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
RegisterPlugin	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
Restore	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
RollbackDeployment	Global Objects	Manage Deployment Groups	Read and Write on destination folder
Run	-	-	-
ShowConnectionInfo	-	-	-
SwitchConnection	Run-time Objects	Create, Edit, and Delete	Read and Write on folder Read on connection object
TruncateLog	Run-time Objects	Manage Execution	Read and Execute on folder
UndoCheckout (for your own checkouts)	Design Objects	Create, Edit, and Delete	Read and Write on folder
UndoCheckout (for your own checkouts)	Sources and Targets	Create, Edit, and Delete	Read and Write on folder
UndoCheckout (for your own checkouts)	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
UndoCheckout (for others' checkouts)	Design Objects	Manage Versions	Read and Write on folder
UndoCheckout (for others' checkouts)	Sources and Targets	Manage Versions	Read and Write on folder
UndoCheckout (for others' checkouts)	Run-time Objects	Manage Versions	Read and Write on folder
Unregister	Domain Administration	Manage Services	Permission on PowerCenter Repository Service

pmrep Command	Privilege Group	Privilege Name	Permission
UnregisterPlugin	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
UpdateConnection	-	-	Read and Write on connection object
UpdateEmailAddr	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
UpdateSeqGenVals	Design Objects	Create, Edit, and Delete	Read and Write on folder
UpdateSrcPrefix	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
UpdateStatistics	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
UpdateTargPrefix	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
Upgrade	Domain Administration	Manage Services	Permission on PowerCenter Repository Service
Validate	Design Objects	Create, Edit, and Delete	Read and Write on folder
Validate	Run-time Objects	Create, Edit, and Delete	Read and Write on folder
Version	-	-	-

APPENDIX C

Custom Roles

This appendix includes the following topics:

- [PowerCenter Repository Service Custom Roles, 284](#)
- [Metadata Manager Service Custom Roles, 286](#)
- [Reporting Service Custom Roles, 287](#)
- [Test Data Manager Service Custom Roles, 294](#)
- [Analyst Service Custom Role, 297](#)

PowerCenter Repository Service Custom Roles

The following table lists the default privileges assigned to the PowerCenter Connection Administrator custom role:

Privilege Group	Privilege Name
Tools	Access Workflow Manager
Global Objects	Create Connections

The following table lists the default privileges assigned to the PowerCenter Developer custom role:

Privilege Group	Privilege Name
Tools	<ul style="list-style-type: none">- Access Designer- Access Workflow Manager- Access Workflow Monitor
Design Objects	<ul style="list-style-type: none">- Create, Edit, and Delete- Manage Versions

Privilege Group	Privilege Name
Sources and Targets	<ul style="list-style-type: none"> - Create, Edit, and Delete - Manage Versions
Run-time Objects	<ul style="list-style-type: none"> - Create, Edit, and Delete - Execute - Manage Versions - Monitor

The following table lists the default privileges assigned to the PowerCenter Operator custom role:

Privilege Group	Privilege Name
Tools	Access Workflow Monitor
Run-time Objects	<ul style="list-style-type: none"> - Execute - Manage Execution - Monitor

The following table lists the default privileges assigned to the PowerCenter Repository Folder Administrator custom role:

Privilege Group	Privilege Name
Tools	Access Repository Manager
Folders	<ul style="list-style-type: none"> - Copy - Create - Manage Versions
Global Objects	<ul style="list-style-type: none"> - Manage Deployment Groups - Execute Deployment Groups - Create Labels - Create Queries

Metadata Manager Service Custom Roles

Metadata Manager Service custom roles include the Metadata Manager Advanced User, Metadata Manager Basic User, and Metadata Manager Intermediate User roles.

The following table lists the default privileges assigned to the Metadata Manager Advanced User custom role:

Privilege Group	Privilege Name
Catalog	<ul style="list-style-type: none">- Share Shortcuts- View Lineage- View Related Catalogs- View Reports- View Profile Results- View Catalog- View Relationships- Manage Relationships- View Comments- Post Comments- Delete Comments- View Links- Manage Links- View Glossary- Manage Objects
Load	<ul style="list-style-type: none">- View Resource- Load Resource- Manage Schedules- Purge Metadata- Manage Resource
Model	<ul style="list-style-type: none">- View Model- Manage Model- Export/Import Models
Security	Manage Catalog Permissions

The following table lists the default privileges assigned to the Metadata Manager Basic User custom role:

Privilege Group	Privilege Name
Catalog	<ul style="list-style-type: none">- View Lineage- View Related Catalogs- View Catalog- View Relationships- View Comments- View Links
Model	View Model

The following table lists the default privileges assigned to the Metadata Manager Intermediate User custom role:

Privilege Group	Privilege Name
Catalog	<ul style="list-style-type: none"> - View Lineage - View Related Catalogs - View Reports - View Profile Results - View Catalog - View Relationships - View Comments - Post Comments - Delete Comments - View Links - Manage Links - View Glossary
Load	<ul style="list-style-type: none"> - View Resource - Load Resource
Model	View Model

Reporting Service Custom Roles

The following table lists the default privileges assigned to the Reporting Service Advanced Consumer custom role:

Privilege Group	Privilege Name
Administration	<ul style="list-style-type: none"> - Maintain Schema - Export/Import XML Files - Manage User Access - Set Up Schedules and Tasks - Manage System Properties - Set Up Query Limits - Configure Real-time Message Streams
Alerts	<ul style="list-style-type: none"> - Receive Alerts - Create Real-time Alerts - Set up Delivery Options

Privilege Group	Privilege Name
Communication	<ul style="list-style-type: none"> - Print - Email Object Links - Email Object Contents - Export - Export to Excel or CSV - Export to Pivot Table - View Discussions - Add Discussions - Manage Discussions - Give Feedback
Content Directory	<ul style="list-style-type: none"> - Access Content Directory - Access Advanced Search - Manage Content Directory - Manage Advanced Search
Dashboard	<ul style="list-style-type: none"> - View Dashboards - Manage Personal Dashboards
Indicators	<ul style="list-style-type: none"> - Interact with Indicators - Create Real-time Indicators - Get Continuous, Automatic Real-time Indicator Updates
Manage Accounts	Manage Personal Settings
Reports	<ul style="list-style-type: none"> - View Reports - Analyze Reports - Interact with Data - Drill Anywhere - Create Filtersets - Promote Custom Metric - View Query - View Life Cycle Metadata - Create and Delete Reports - Access Basic Report Creation - Access Advanced Report Creation - Save Copy of Reports - Edit Reports

The following table lists the default privileges assigned to the Reporting Service Advanced Provider custom role:

Privilege Group	Privilege Name
Administration	Maintain Schema
Alerts	<ul style="list-style-type: none"> - Receive Alerts - Create Real-time Alerts - Set Up Delivery Options
Communication	<ul style="list-style-type: none"> - Print - Email Object Links - Email Object Contents - Export - Export to Excel or CSV - Export to Pivot Table - View Discussions - Add Discussions - Manage Discussions - Give Feedback
Content Directory	<ul style="list-style-type: none"> - Access Content Directory - Access Advanced Search - Manage Content Directory - Manage Advanced Search
Dashboards	<ul style="list-style-type: none"> - View Dashboards - Manage Personal Dashboards - Create, Edit, and Delete Dashboards - Access Basic Dashboard Creation - Access Advanced Dashboard Creation
Indicators	<ul style="list-style-type: none"> - Interact With Indicators - Create Real-time Indicators - Get Continuous, Automatic Real-time Indicator Updates

Privilege Group	Privilege Name
Manage Accounts	Manage Personal Settings
Reports	<ul style="list-style-type: none"> - View Reports - Analyze Reports - Interact with Data - Drill Anywhere - Create Filtersets - Promote Custom Metric - View Query - View Life Cycle Metadata - Create and Delete Reports - Access Basic Report Creation - Access Advanced Report Creation - Save Copy of Reports - Edit Reports

The following table lists the default privileges assigned to the Reporting Service Basic Consumer custom role:

Privilege Group	Privilege Name
Alerts	<ul style="list-style-type: none"> - Receive Alerts - Set Up Delivery Options
Communication	<ul style="list-style-type: none"> - Print - Email Object Links - Export - View Discussions - Add Discussions - Give Feedback
Content Directory	Access Content Directory
Dashboards	View Dashboards
Manage Account	Manage Personal Settings
Reports	<ul style="list-style-type: none"> - View Reports - Analyze Reports

The following table lists the default privileges assigned to the Reporting Service Basic Provider custom role:

Privilege Group	Privilege Name
Administration	Maintain Schema
Alerts	<ul style="list-style-type: none"> - Receive Alerts - Create Real-time Alerts - Set Up Delivery Options
Communication	<ul style="list-style-type: none"> - Print - Email Object Links - Email Object Contents - Export - Export To Excel or CSV - Export To Pivot Table - View Discussions - Add Discussions - Manage Discussions - Give Feedback
Content Directory	<ul style="list-style-type: none"> - Access Content Directory - Access Advanced Search - Manage Content Directory - Manage Advanced Search
Dashboards	<ul style="list-style-type: none"> - View Dashboards - Manage Personal Dashboards - Create, Edit, and Delete Dashboards - Access Basic Dashboard Creation
Indicators	<ul style="list-style-type: none"> - Interact with Indicators - Create Real-time Indicators - Get Continuous, Automatic Real-time Indicator Updates

Privilege Group	Privilege Name
Manage Accounts	Manage Personal Settings
Reports	<ul style="list-style-type: none"> - View Reports - Analyze Reports - Interact with Data - Drill Anywhere - Create Filtersets - Promote Custom Metric - View Query - View Life Cycle Metadata - Create and Delete Reports - Access Basic Report Creation - Access Advanced Report Creation - Save Copy of Reports - Edit Reports

The following table lists the default privileges assigned to the Reporting Service Intermediate Consumer custom role:

Privilege Group	Privilege Name
Alerts	<ul style="list-style-type: none"> - Receive Alerts - Set Up Delivery Options
Communication	<ul style="list-style-type: none"> - Print - Email Object Links - Export - Export to Excel or CSV - Export to Pivot Table - View Discussions - Add Discussions - Manage Discussions - Give Feedback
Content Directory	Access Content Directory
Dashboards	<ul style="list-style-type: none"> - View Dashboards - Manage Personal Dashboards
Indicators	<ul style="list-style-type: none"> - Interact with Indicators - Get Continuous, Automatic Real-time Indicator Updates

Privilege Group	Privilege Name
Manage Accounts	Manage Personal Settings
Reports	<ul style="list-style-type: none"> - View Reports - Analyze Reports - Interact with Data - View Life Cycle Metadata - Save Copy of Reports

The following table lists the default privileges assigned to the Reporting Service Read Only Consumer custom role:

Privilege Group	Privilege Name
Reports	View Reports

The following table lists the default privileges assigned to the Reporting Service Schema Designer custom role:

Privilege Group	Privilege Name
Administration	<ul style="list-style-type: none"> - Maintain Schema - Set Up Schedules and Tasks - Configure Real-time Message Streams
Alerts	<ul style="list-style-type: none"> - Receive Alerts - Create Real-time Alerts - Set Up Delivery Options
Communication	<ul style="list-style-type: none"> - Print - Email Object Links - Email Object Contents - Export - Export to Excel or CSV - Export to Pivot Table - View Discussions - Add Discussions - Manage Discussions - Give Feedback
Content Directory	<ul style="list-style-type: none"> - Access Content Directory - Access Advanced Search - Manage Content Directory - Manage Advanced Search

Privilege Group	Privilege Name
Dashboards	<ul style="list-style-type: none"> - View Dashboards - Manage Personal Dashboards - Create, Edit, and Delete Dashboards
Indicators	<ul style="list-style-type: none"> - Interact with Indicators - Create Real-time Indicators - Get Continuous, Automatic Real-time Indicator Updates
Manage Accounts	Manage Personal Settings
Reports	<ul style="list-style-type: none"> - View Reports - Analyze Reports - Interact with Data - Drill Anywhere - Create Filtersets - Promote Custom Metric - View Query - View Life Cycle Metadata - Create and Delete Reports - Access Basic Report Creation - Access Advanced Report Creation - Save Copy of Reports - Edit Reports

Test Data Manager Service Custom Roles

The following table lists the default privileges assigned to the Test Data Administrator custom role:

Privilege Group	Privilege Name
Projects	Audit Project
Administration	<ul style="list-style-type: none"> - View Connections - Manage Connections

The following table lists the default privileges assigned to the Test Data Developer custom role:

Privilege Group	Privilege Name
Policies	<ul style="list-style-type: none"> - View Policies - Manage Policies
Rules	<ul style="list-style-type: none"> - View Masking Rules - Manage Masking Rules - View Generation Rules
Data Domains	<ul style="list-style-type: none"> - View Data Domains - Manage Data Domains
Projects	Audit project

The following table lists the default privileges assigned to the Test Data Project DBA custom role:

Privilege Group	Privilege Name
Projects	<ul style="list-style-type: none"> - View Project - Execute Project - Monitor Project - Audit Project
Administration	<ul style="list-style-type: none"> - View Connections - Manage Connections

The following table lists the default privileges assigned to the Test Data Project Developer custom role:

Privilege Group	Privilege Name
Policies	View Policies
Rules	<ul style="list-style-type: none"> - View Masking Rules - View Generation Rules
Data Domains	View Data Domains
Projects	<ul style="list-style-type: none"> - View Project - Discover Project - Execute Project - Monitor Project - Audit Project - Import Metadata
Data Masking	<ul style="list-style-type: none"> - View Data Masking - Manage Data Masking
Data Subset	<ul style="list-style-type: none"> - View Data Subset - Manage Data Subset

Privilege Group	Privilege Name
Data Generation	<ul style="list-style-type: none"> - View Data Generation - Manage Data Generation
Administration	<ul style="list-style-type: none"> - View Connections - Manage Connections

The following table lists the default privileges assigned to the Test Data Project Owner custom role:

Privilege Group	Privilege Name
Policies	View Policies
Rules	<ul style="list-style-type: none"> - View Masking Rules - View Generation Rules
Data Domains	View Data Domains
Projects	<ul style="list-style-type: none"> - View Project - Manage Project - Discover Project - Execute Project - Monitor Project - Audit Project - Import Metadata
Data Masking	<ul style="list-style-type: none"> - View Data Masking - Manage Data Masking
Data Subset	<ul style="list-style-type: none"> - View Data Subset - Manage Data Subset
Data Generation	<ul style="list-style-type: none"> - View Data Generation - Manage Data Generation
Administration	<ul style="list-style-type: none"> - View Connections - Manage Connections

The following table lists the default privileges assigned to the Test Data Risk Manager custom role:

Privilege Group	Privilege Name
Policies	View Policies
Rules	<ul style="list-style-type: none"> - View Masking Rules - View Generation Rules
Data Domains	View Data Domains
Projects	Audit project

The following table lists the default privileges assigned to the Test Data Specialist custom role:

Privilege Group	Privilege Name
Policies	View Policies
Rules	<ul style="list-style-type: none">- View Masking Rules- Manage Masking Rules- View Generation Rules- Manage Generation Rules
Data Domains	<ul style="list-style-type: none">- View Data Domains- Manage Data Domains
Projects	<ul style="list-style-type: none">- Manage Project- View Project- Discover Project- Execute Project- Monitor Project- Audit Project- Import Metadata
Data Masking	<ul style="list-style-type: none">- View Data Masking- Manage Data Masking
Data Subset	<ul style="list-style-type: none">- View Data Subset- Manage Data Subset
Data Generation	<ul style="list-style-type: none">- View Data Generation- Manage Data Generation
Administration	<ul style="list-style-type: none">- View Connections- Manage Connections

Note: If your TDM setup uses Informatica service 9.6.1, or if you have upgraded to Informatica service 9.6.1 HotFix 1, a user with the Test Data Specialist role cannot create or delete data generation rules. The role does not include the Manage Data Generation privilege. To enable users with this role to create and delete data generation rules, you must manually edit the role. Log in to the Administrator tool and edit the TDM service custom role to include the Manage Generation Rules privilege from the Rules privilege group.

Analyst Service Custom Role

The Analyst Service Business Glossary Consumer is a custom Analyst Service role.

The following table lists the default privilege assigned to the Analyst Service Business Glossary Consumer custom role:

Privilege Group	Privilege Name
Workspace Access	Glossary Workspace

APPENDIX D

Informatica Platform Connectivity

This appendix includes the following topics:

- [Informatica Platform Connectivity Overview, 298](#)
- [Domain Connectivity, 299](#)
- [PowerCenter Connectivity, 301](#)
- [Native Connectivity, 306](#)
- [ODBC Connectivity, 306](#)
- [JDBC Connectivity, 307](#)

Informatica Platform Connectivity Overview

The Informatica platform uses the following types of connectivity to communicate among clients, services, and other components in the domain:

TCP/IP network protocol

Application services and the Service Managers in a domain use TCP/IP network protocol to communicate with other nodes and services. The clients also use TCP/IP to communicate with application services. You can configure the host name and port number for TCP/IP communication on a node when you install the Informatica services. You can configure the port numbers used for services on a node during installation or in Informatica Administrator.

Native drivers

The Data Integration Service uses native drivers to communicate with databases. The PowerCenter Integration Service and the PowerCenter Repository Service use native drivers to communicate with databases. Native drivers are packaged with the database server and client software. Install and configure the native database client software on the machines where the services run.

ODBC

The ODBC drivers are installed with the Informatica services and the Informatica clients. The integration services use ODBC drivers to communicate with databases.

JDBC

The Model Repository Service uses JDBC to connect to the Model repository database. The Reporting Service uses JDBC to connect to the Data Analyzer repository and data sources. The Metadata Manager Service uses JDBC to connect to the Metadata Manager repository and metadata source repositories.

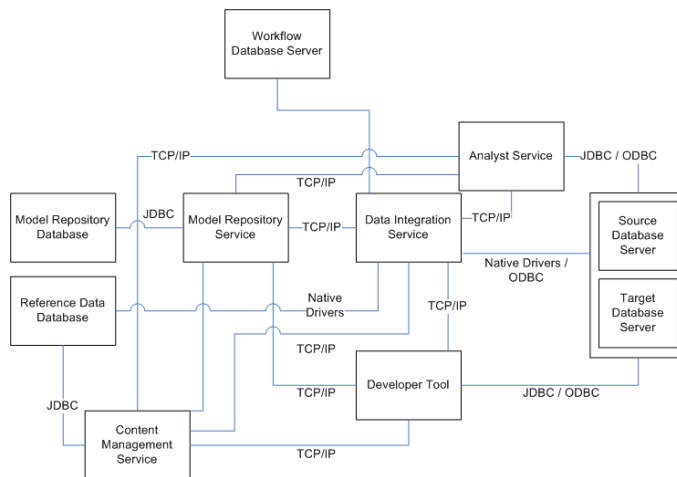
The gateway nodes in the Informatica domain use JDBC to connect to the domain configuration repository.

Domain Connectivity

Services on a node in an Informatica domain use TCP/IP to connect to services on other nodes. Because services can run on multiple nodes in the domain, services rely on the Service Manager to route requests. The Service Manager on the master gateway node handles requests for services and responds with the address of the requested service.

Nodes communicate through TCP/IP on the port you select for a node when you install Informatica Services. When you create a node, you select a port number for the node. The Service Manager listens for incoming TCP/IP connections on that port.

The following figure shows an overview of the connectivity for components in the platform:



The platform uses connection objects to define connectivity information for source and target databases. The connection objects can use native or ODBC connectivity. The Data Integration Service uses connection objects to connect to sources and targets.

The services and clients connect in the following ways:

Model Repository Service

The Model Repository Service uses JDBC to read or write data and metadata in the Model repository. It uses TCP/IP to communicate with the Data Integration Service and the clients.

Data Integration Service

The Data Integration Service uses ODBC or native drivers to connect and read data from a source database and write data to a target database. It uses TCP/IP to communicate with the Model Repository Service, Content Management Service, and client applications.

Informatica Developer

The Developer tool uses TCP/IP to send data transformation requests to the Data Integration Service. It uses TCP/IP to communicate with the Content Management Service to manage reference tables, probabilistic model files, and to retrieve configuration and status information for identity population files and address validation reference data files. When you preview mappings or data objects in the Developer tool, it uses JDBC or ODBC drivers to connect to the source or target database to fetch the metadata required for preview.

Informatica Analyst

The Analyst tool uses TCP/IP to send requests to the Data Integration Service. It uses TCP/IP to communicate with the Content Management Service to manage reference tables. When you preview

profiles or objects in the Analyst tool, it uses JDBC or ODBC drivers to connect to the source or target database to fetch the metadata required for preview.

If you use ODBC to connect to the source or target database, install the ODBC driver on the node where the Analyst Service runs.

Content Management Service

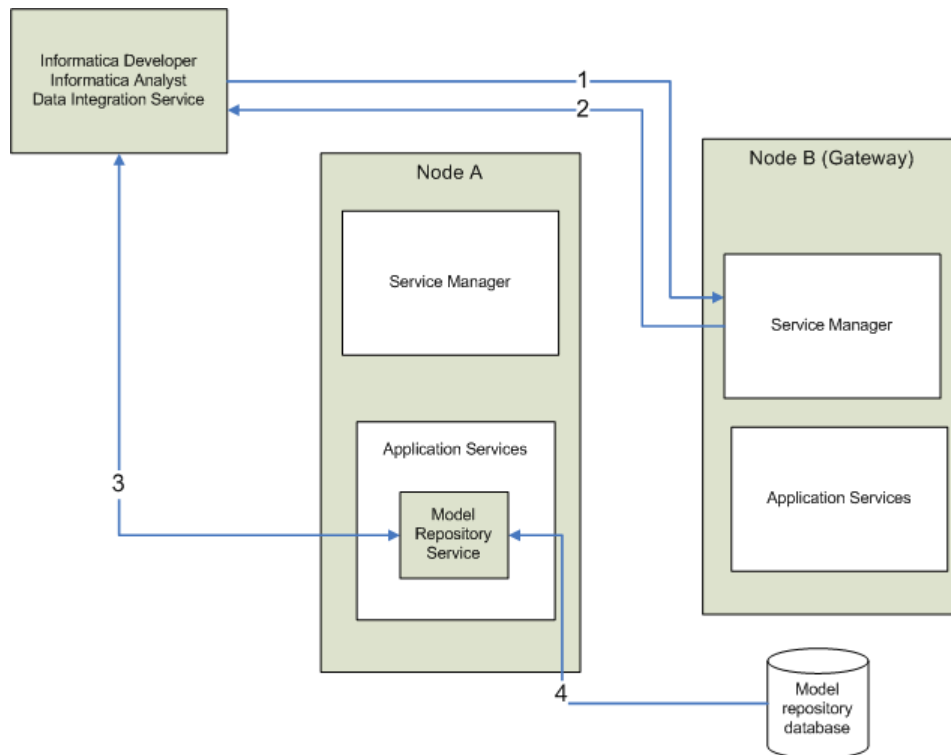
The Content Management Service manages the locations and other properties for reference data. The Content Management Service uses TCP/IP to communicate with the Data Integration Service to read and write data in reference tables. It uses JDBC to communicate directly with the reference data warehouse when it creates the reference tables.

If multiple instances of a Content Management Service exist in an Informatica domain, the master Content Management Service updates the Data Integration Service. The master Content Management Service uses TCP/IP to communicate with the Domain Service to identify the Model Repository Service and Data Integration Service to use.

Model Repository Connectivity

The Model Repository Service connects to the Model repository using JDBC drivers. Informatica Developer, Informatica Analyst, Informatica Administrator, and the Data Integration Service communicate with the Model Repository Service over TCP/IP. Informatica Developer, Informatica Analyst, and Data Integration Service are Model repository clients.

The following figure shows how a Model repository client connects to the Model repository database:



1. A Model repository client sends a repository connection request to the master gateway node, which is the entry point to the domain.
2. The Service Manager sends back the host name and port number of the node running the Model Repository Service. In the diagram, the Model Repository Service is running on node A.
3. The repository client establishes a TCP/IP connection with the Model Repository Service process on node A.
4. The Model Repository Service process communicates with the Model repository database over JDBC. The Model Repository Service process stores objects in or retrieves objects from the Model repository database based on requests from the Model repository client.

Note: The Model repository tables have an open architecture. Although you can view the repository tables, never manually edit them through other utilities. Informatica is not responsible for corrupted data that is caused by customer alteration of the repository tables or data within those tables.

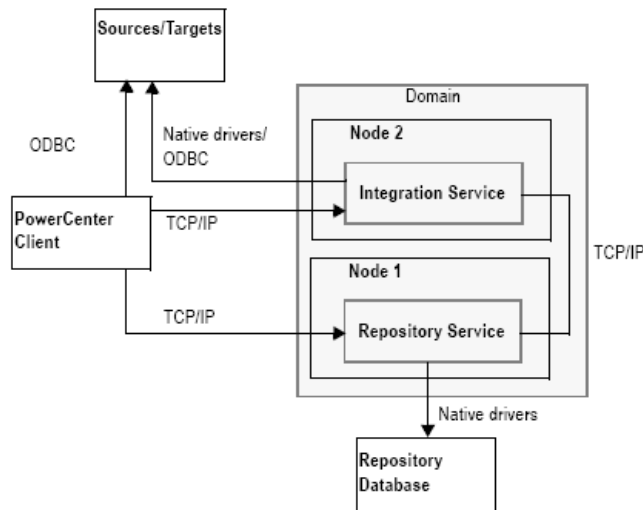
PowerCenter Connectivity

PowerCenter uses the TCP/IP network protocol, native database drivers, ODBC, and JDBC for communication between the following PowerCenter components:

- **PowerCenter Repository Service.** The PowerCenter Repository Service uses native database drivers to communicate with the PowerCenter repository. The PowerCenter Repository Service uses TCP/IP to communicate with other PowerCenter components.
- **PowerCenter Integration Service.** The PowerCenter Integration Service uses native database connectivity and ODBC to connect to source and target databases. The PowerCenter Integration Service uses TCP/IP to communicate with other PowerCenter components.
- **Reporting Service and Metadata Manager Service.** Data Analyzer and Metadata Manager use JDBC and ODBC to access data sources and repositories.

- **PowerCenter Client.** PowerCenter Client uses ODBC to connect to source and target databases. PowerCenter Client uses TCP/IP to communicate with the PowerCenter Repository Service and PowerCenter Integration Service.

The following figure shows an overview of PowerCenter components and connectivity:



The following table lists the drivers used by PowerCenter components:

Component	Database	Driver
PowerCenter Repository Service	PowerCenter Repository	Native
PowerCenter Integration Service	Source Target Stored Procedure Lookup	Native ODBC
Reporting Service	Data Analyzer Repository	JDBC
Reporting Service	Data Source	JDBC ODBC with JDBC-ODBC bridge
Metadata Manager Service	Metadata Manager Repository	JDBC
PowerCenter Client	PowerCenter Repository	Native
PowerCenter Client	Source Target Stored Procedure Lookup	ODBC
Custom Metadata Configurator (Metadata Manager client)	Metadata Manager Repository	JDBC

Repository Service Connectivity

The PowerCenter Repository Service manages the metadata in the PowerCenter repository database. All applications that connect to the repository must connect to the PowerCenter Repository Service. The PowerCenter Repository Service uses native drivers to communicate with the repository database.

The following table describes the connectivity required to connect the Repository Service to the repository and source and target databases:

Repository Service Connection	Connectivity Requirement
PowerCenter Client	TCP/IP
PowerCenter Integration Service	TCP/IP
PowerCenter Repository database	Native database drivers

The PowerCenter Integration Service connects to the Repository Service to retrieve metadata when it runs workflows.

Connecting from PowerCenter Client

To connect to the PowerCenter Repository Service from PowerCenter Client, add a domain and repository in the PowerCenter Client tool. When you connect to the repository from a PowerCenter Client tool, the client tool sends a connection request to the Service Manager on the gateway node. The Service Manager returns the host name and port number of the node where the PowerCenter Repository Service runs. PowerCenter Client uses TCP/IP to connect to the PowerCenter Repository Service.

Connecting to Databases

To set up a connection from the PowerCenter Repository Service to the repository database, configure the database properties in Informatica Administrator. You must install and configure the native database drivers for the repository database on the machine where the PowerCenter Repository Service runs.

Integration Service Connectivity

The PowerCenter Integration Service connects to the repository to read repository objects. The PowerCenter Integration Service connects to the repository through the PowerCenter Repository Service. Use Informatica Administrator to configure an associated repository for the Integration Service.

The following table describes the connectivity required to connect the PowerCenter Integration Service to the platform components, source databases, and target databases:

PowerCenter Integration Service Connection	Connectivity Requirement
PowerCenter Client	TCP/IP
Other PowerCenter Integration Service Processes	TCP/IP

PowerCenter Integration Service Connection	Connectivity Requirement
Repository Service	TCP/IP
Source and target databases	Native database drivers or ODBC Note: The PowerCenter Integration Service on Windows and UNIX can use ODBC drivers to connect to databases. You can use native drivers to improve performance.

The PowerCenter Integration Service includes ODBC libraries that you can use to connect to other ODBC sources. The Informatica installation includes ODBC drivers.

For flat file, XML, or COBOL sources, you can either access data with network connections, such as NFS, or transfer data to the PowerCenter Integration Service node through FTP software. For information about connectivity software for other ODBC sources, refer to your database documentation.

Connecting from the PowerCenter Client

The Workflow Manager communicates with a PowerCenter Integration Service process over a TCP/IP connection. The Workflow Manager communicates with the PowerCenter Integration Service process each time you start a workflow or display workflow details.

Connecting to the PowerCenter Repository Service

When you create a PowerCenter Integration Service, you specify the PowerCenter Repository Service to associate with the PowerCenter Integration Service. When the PowerCenter Integration Service runs a workflow, it uses TCP/IP to connect to the associated PowerCenter Repository Service and retrieve metadata.

Connecting to Databases

Use the Workflow Manager to create connections to databases. You can create connections using native database drivers or ODBC. If you use native drivers, specify the database user name, password, and native connection string for each connection. The PowerCenter Integration Service uses this information to connect to the database when it runs the session.

Note: PowerCenter supports ODBC drivers, such as ISG Navigator, that do not need user names and passwords to connect. To avoid using empty strings or nulls, use the reserved words PmNullUser and PmNullPasswd for the user name and password when you configure a database connection. The PowerCenter Integration Service treats PmNullUser and PmNullPasswd as no user and no password.

PowerCenter Client Connectivity

The PowerCenter Client uses ODBC drivers and native database client connectivity software to communicate with databases. It uses TCP/IP to communicate with the Integration Service and with the repository.

The following table describes the connectivity types required to connect the PowerCenter Client to the Integration Service, repository, and source and target databases:

PowerCenter Client Connection	Connectivity Requirement
Integration Service	TCP/IP
Repository Service	TCP/IP
Databases	ODBC connection for each database

Connecting to the Repository

You can connect to the repository using the PowerCenter Client tools. All PowerCenter Client tools use TCP/IP to connect to the repository through the Repository Service each time you access the repository to perform tasks such as connecting to the repository, creating repository objects, and running object queries.

Connecting to Databases

To connect to databases from the Designer, use the Windows ODBC Data Source Administrator to create a data source for each database you want to access. Select the data source names in the Designer when you perform the following tasks:

- **Import a table or a stored procedure definition from a database.** Use the Source Analyzer or Target Designer to import the table from a database. Use the Transformation Developer, Maplet Designer, or Mapping Designer to import a stored procedure or a table for a Lookup transformation.
To connect to the database, you must also provide your database user name, password, and table or stored procedure owner name.
- **Preview data.** You can select the data source name when you preview data in the Source Analyzer or Target Designer. You must also provide your database user name, password, and table owner name.

Connecting to the Integration Service

The Workflow Manager and Workflow Monitor communicate directly with the Integration Service over TCP/IP each time you perform session and workflow-related tasks, such as running a workflow. When you log in to a repository through the Workflow Manager or Workflow Monitor, the client application lists the Integration Services that are configured for that repository in Informatica Administrator.

Reporting Service and Metadata Manager Service Connectivity

To connect to a Data Analyzer repository, the Reporting Service requires a Java Database Connectivity (JDBC) driver. To connect to the data source, the Reporting Service can use a JDBC driver or a JDBC-ODBC bridge with an ODBC driver.

To connect to a Metadata Manager repository, the Metadata Manager Service requires a JDBC driver. The Custom Metadata Configurator uses a JDBC driver to connect to the Metadata Manager repository.

JDBC drivers are installed with the Informatica services and the Informatica clients. You can use the installed JDBC drivers to connect to the Data Analyzer or Metadata Manager repository, data source, or to a PowerCenter repository.

The Informatica installers do not install ODBC drivers or the JDBC-ODBC bridge for the Reporting Service or Metadata Manager Service.

Native Connectivity

To establish native connectivity between an application service and a database, you must install the database client software on the machine where the service runs.

The Data Integration Service uses native drivers to communicate with source and target databases.

The PowerCenter Integration Service and PowerCenter Repository Service use native drivers to communicate with source and target databases and repository databases.

The following table describes the syntax for the native connection string for each supported database system:

Database	Connect String Syntax	Example
IBM DB2	<i>dbname</i>	mydatabase
Informix	<i>dbname@servername</i>	mydatabase@informix
Microsoft SQL Server	<i>servername@dbname</i>	sqlserver@mydatabase
Oracle	<i>dbname.world</i> (same as TNSNAMES entry)	oracle.world
Sybase ASE	<i>servername@dbname</i>	sambrown@mydatabase Note: Sybase ASE servername is the name of the Adaptive Server from the interfaces file.
Teradata	<i>ODBC_data_source_name</i> or <i>ODBC_data_source_name@db_name</i> or <i>ODBC_data_source_name@db_user_name</i>	TeradataODBC TeradataODBC@mydatabase TeradataODBC@sambrown Note: Use Teradata ODBC drivers to connect to source and target databases.

ODBC Connectivity

Open Database Connectivity (ODBC) provides a common way to communicate with different database systems.

The Data Integration Service use ODBC drivers to connect to databases.

PowerCenter Client uses ODBC drivers to connect to source, target, and lookup databases and call the stored procedures in databases. The PowerCenter Integration Service can also use ODBC drivers to connect to databases.

To use ODBC connectivity, you must install the following components on the machine hosting the Informatica service or client tool:

- **Database client software.** Install the client software for the database system. This installs the client libraries needed to connect to the database.

Note: Some ODBC drivers contain wire protocols and do not require the database client software.

- **ODBC drivers.** The DataDirect closed 32-bit or 64-bit ODBC drivers are installed when you install the Informatica services. The DataDirect closed 32-bit ODBC drivers are installed when you install the Informatica clients. The database server can also include an ODBC driver.

After you install the necessary components you must configure an ODBC data source for each database that you want to connect to. A data source contains information that you need to locate and access the database, such as database name, user name, and database password. On Windows, you use the ODBC Data Source Administrator to create a data source name. On UNIX, you add data source entries to the `odbc.ini` file found in the system `$ODBCHOME` directory.

When you create an ODBC data source, you must also specify the driver that the ODBC driver manager sends database calls to.

The following table shows the recommended ODBC drivers to use with each database:

Database	ODBC Driver	Requires Database Client Software
Informix	DataDirect Informix Wire Protocol	No
Microsoft Access	Microsoft Access driver	No
Microsoft Excel	Microsoft Excel driver	No
Microsoft SQL Server	DataDirect SQL Server Wire Protocol	No
Netezza	Netezza SQL	Yes
Teradata	Teradata ODBC driver	Yes
SAP HANA	SAP HANA ODBC driver	Yes

JDBC Connectivity

JDBC (Java Database Connectivity) is a Java API that provides connectivity to relational databases. Java-based applications can use JDBC drivers to connect to databases.

The following services and clients use JDBC to connect to databases:

- Data Integration Service
- Model Repository Service
- Informatica Developer
- Informatica Analyst
- Metadata Manager Service
- Reporting Service
- Custom Metadata Configurator

JDBC drivers are installed with the Informatica services and the Informatica clients.

APPENDIX E

Configure the Web Browser

This appendix includes the following topic:

- [Configure the Web Browser, 308](#)

Configure the Web Browser

You can run the Administrator tool on the Microsoft Internet Explorer or Google Chrome web browser.

To use the Administrator tool, configure the following options in the browser:

Scripting and ActiveX

Enable the following controls on Microsoft Internet Explorer:

- Active scripting
- Allow programmatic clipboard access
- Run ActiveX controls and plug-ins
- Script ActiveX controls marked safe for scripting

To configure the controls, click **Tools > Internet options > Security > Custom level**.

Adobe Flash Player Plug-In

Informatica Administrator contains the Dependency Graph window, which requires the Adobe Flash Player plug-in version 10 or later. To view dependencies for application services and nodes in the Dependency Graph, download and install the Flash Player plug-in on the web browser. Get the Flash Player plug-in from the following web site: www.adobe.com/products/flashplayer

TLS 1.0

If you configure HTTPS for Informatica Administrator on a domain that runs on AIX, Internet Explorer requires TLS 1.0. To enable TLS 1.0, click **Tools > Internet Options > Advanced**. The TLS 1.0 setting is listed below the Security heading.

Trusted sites

If the Informatica domain runs on a network with Kerberos authentication, you must configure the browser to allow access to the Informatica web applications. In Microsoft Internet Explorer and Google Chrome, add the URL of the Informatica web application to the list of trusted sites. If you are using Chrome version 41 or later, you must also set the `AuthServerWhitelist` and `AuthNegotiateDelegateWhitelist` policies.

APPENDIX F

Security Concepts

This appendix includes the following topics:

- [What is a group?, 309](#)
- [What is a user?, 309](#)
- [What is a role?, 310](#)
- [What is a privilege?, 310](#)
- [What is an operating system profile?, 310](#)

What is a group?

A group is a collection of users and groups that can have the same permissions and privileges. An Informatica domain can have native or LDAP groups. When you assign a role, permission, or privilege to a group, you assign all users and subgroups within the group the same role, permission, and privilege.

Groups in a native security domain are called native groups. You can use Informatica Administrator to create and manage native groups. A native group can have native and LDAP user accounts.

Groups in an LDAP security domain are called LDAP groups. You create and manage LDAP groups in the LDAP directory service. You cannot create or delete LDAP groups or change LDAP group assignments in Informatica Administrator.

What is a user?

A user is someone who has a user account in the Informatica domain. A user with an account in the Informatica domain can perform tasks in application clients.

Users in a native security domain are called native users. You can use Informatica Administrator to create and manage native user accounts.

Users in an LDAP security domain are called LDAP users. You create and manage LDAP user accounts in the LDAP directory service. You cannot create or delete LDAP users or change LDAP user assignments in Informatica Administrator.

What is a role?

A role is a collection of privileges you can assign to users and groups. You can assign a system-defined role or create and assign your own custom roles to users and groups.

A system-defined role is a role that you cannot edit or delete. The Administrator role is a system-defined role.

A custom role is a role that you can create, edit, and delete.

What is a privilege?

Privileges determine the actions that users can perform in application clients. You assign privileges to users and groups for the domain and for each of the following application services in the domain: Metadata Manager Service, Model Repository Service, PowerCenter Repository Service, and Reporting Service.

You can also assign roles to users and groups to determine the actions that users can perform. A role is a collection of privileges.

What is an operating system profile?

An operating system profile is a level of security that the PowerCenter Integration Service uses to run workflows. The operating system profile contains the operating system user name, service process variables, and environment variables. The PowerCenter Integration Service runs the workflow with the system permissions of the operating system user and settings defined in the operating system profile. If the PowerCenter Integration Service uses operating system profiles, assign operating system profiles to workflows when you define folder properties or when you manually start a workflow. To start a workflow that has an operating system user assigned to it, you must have permission on the operating system profile the PowerCenter Integration Service uses to run the workflow.

INDEX

A

- accounts
 - changing the password [27](#)
 - managing [25](#)
- activity data
 - Web Services Report [208](#)
- Adabas connections
 - properties [88](#)
- Administrator tool
 - code page [228](#)
 - log errors, viewing [166](#)
 - logs, viewing [161](#)
 - reports [200](#)
- alerts
 - configuring [47](#)
 - description [18](#)
 - managing [47](#)
 - notification email [48](#)
 - subscribing to [48](#)
 - tracking [48](#)
 - viewing [48](#)
- Analyst Service
 - application service [33](#)
 - custom roles [297](#)
 - log events [168](#)
- application service process
 - disabling [52](#)
 - enabling [52](#)
 - failed state [52](#)
 - port assignment [19](#)
 - standby state [52](#)
 - state [52](#)
 - stopped state [52](#)
- application services
 - Analyst Service [33](#)
 - Content Management Service [33](#)
 - Data Integration Service [33](#)
 - dependencies [65](#)
 - description [19](#)
 - disabling [52](#)
 - enabling [52](#)
 - licenses, assigning [152](#)
 - licenses, unassigning [152](#)
 - Metadata Manager Service [33](#)
 - Model Repository Service [33](#)
 - overview [33](#)
 - PowerCenter Integration Service [33](#)
 - PowerCenter Repository Service [33](#)
 - PowerExchange Listener Service [33](#)
 - PowerExchange Logger Service [33](#)
 - removing [53](#)
 - Reporting and Dashboards Service [33](#)
 - Reporting Service [33](#)
 - resilience, configuring [78](#)
 - SAP BW Service [33](#)

- application services (*continued*)
 - Web Services Hub [33](#)
- application sources
 - code page [229](#)
- application targets
 - code page [230](#)
- applications
 - monitoring [182](#)
- as
 - permissions by command [257](#)
 - privileges by command [257](#)
- ASCII mode
 - overview [222](#)
- authentication
 - log events [167](#)
- authorization
 - log events [167](#)
 - Service Manager [18](#)
- auto-select
 - network high availability [81](#)
- Average Service Time (property)
 - Web Services Report [208](#)
- Avg DTM Time (property)
 - Web Services Report [208](#)
- Avg. No. of Run Instances (property)
 - Web Services Report [208](#)
- Avg. No. of Service Partitions (property)
 - Web Services Report [208](#)

B

- backing up
 - domain configuration database [61](#)
- backup directory
 - node property [55](#)
- BackupDomain command
 - description [61](#)

C

- case study
 - processing ISO 8859-1 data [237](#)
 - processing Unicode UTF-8 data [239](#)
- catalina.out
 - troubleshooting [159](#)
- category
 - domain log events [167](#)
- changing
 - password for user account [27](#)
- character sizes
 - double byte [226](#)
 - multibyte [226](#)
 - single byte [226](#)

- COBOL
 - connectivity [303](#)
- code page relaxation
 - compatible code pages, selecting [235](#)
 - configuring the Integration Service [235](#)
 - data inconsistencies [234](#)
 - overview [234](#)
 - troubleshooting [235](#)
- code page validation
 - overview [233](#)
 - relaxed validation [234](#)
- code pages
 - Administrator tool [228](#)
 - application sources [229](#)
 - application targets [230](#)
 - choosing [226](#)
 - compatibility diagram [231](#)
 - compatibility overview [226](#)
 - conversion [236](#)
 - Custom transformation [231](#)
 - Data Integration Service process [245](#)
 - descriptions [247](#)
 - domain configuration database [227](#)
 - External Procedure transformation [231](#)
 - flat file sources [229](#)
 - flat file targets [230](#)
 - ID [247](#)
 - lookup database [231](#)
 - Metadata Manager Service [229](#)
 - names [247](#)
 - overview [224](#)
 - pmcmd [228](#)
 - PowerCenter Client [228](#)
 - PowerCenter Integration Service process [228](#), [245](#)
 - relational sources [229](#)
 - relational targets [230](#)
 - relationships [233](#)
 - relaxed validation for sources and targets [234](#)
 - repository [229](#), [245](#)
 - sort order overview [228](#)
 - sources [229](#), [247](#)
 - stored procedure database [231](#)
 - supported code pages [245](#), [247](#)
 - targets [230](#), [247](#)
 - UNIX [225](#)
 - validation [233](#)
 - Windows [225](#)
- command line programs
 - privileges [257](#)
 - resilience, configuring [80](#)
- compatibility
 - between code pages [226](#)
 - between source and target code pages [235](#)
- compatible
 - defined for code page compatibility [226](#)
- complete history statistics
 - Web Services Report [211](#)
- Configuration Support Manager
 - using to analyze node diagnostics [218](#)
 - using to review node diagnostics [214](#)
- connect string
 - examples [306](#)
 - syntax [306](#)
- connecting
 - SQL data service [85](#)
- connecting to databases
 - JDBC [305](#)
- connection pooling
 - properties [87](#)
- connection strings
 - native connectivity [306](#)
- connections
 - adding pass-through security [86](#)
 - creating database connections [83](#)
 - deleting [85](#)
 - editing [84](#)
 - overview [82](#)
 - pass-through security [85](#)
 - refreshing [83](#)
 - testing [84](#)
 - web services properties [135](#)
- connectivity
 - COBOL [303](#)
 - connect string examples [306](#)
 - Content Management Service [299](#)
 - Data Analyzer [305](#)
 - Data Integration Service [299](#)
 - diagram of [298](#)
 - Informatica Analyst [299](#)
 - Informatica Developer [299](#)
 - Integration Service [303](#)
 - Metadata Manager [305](#)
 - Model Repository Service [299](#)
 - overview [298](#)
 - PowerCenter Client [304](#)
 - PowerCenter Repository Service [303](#)
 - Content Management Service
 - application service [33](#)
 - connectivity [299](#)
- CPU detail
 - License Management Report [202](#)
- CPU profile
 - node property [55](#)
- CPU summary
 - License Management Report [201](#)
- CPUs
 - exceeding the limit [201](#)
- custom filters
 - date and time [199](#)
 - elapsed time [199](#)
 - multi-select [199](#)
- custom properties
 - domain [71](#)
- custom roles
 - Analyst Service [297](#)
 - Metadata Manager Service [286](#)
 - PowerCenter Repository Service [284](#)
 - Reporting Service [287](#)

D

- Data Analyzer
 - connectivity [305](#)
 - JDBC-ODBC bridge [305](#)
 - ODBC (Open Database Connectivity) [298](#)
- Data Integration Service
 - application service [33](#)
 - connectivity [299](#)
 - log events [168](#)
 - recovery [77](#)
- Data Integration Service process
 - supported code pages [245](#)
- Data Integration Services
 - monitoring [180](#)

- data movement mode
 - ASCII [223](#)
 - changing [223](#)
 - description [222](#)
 - effect on session files and caches [223](#)
 - overview [222](#)
 - Unicode [223](#)
- data object caching
 - with pass-through security [86](#)
- database
 - domain configuration [60](#)
- database connections
 - updating for domain configuration [63](#)
- database drivers
 - Integration Service [298](#)
 - Repository Service [298](#)
- database properties
 - Informatica domain [68](#)
- DataDirect ODBC drivers
 - platform-specific drivers required [306](#)
- DataSift connections
 - properties [90](#)
- deleting
 - connections [85](#)
- dependencies
 - application services [65](#)
 - grids [65](#)
 - nodes [65](#)
 - viewing for services and nodes [65](#)
- deployed mapping jobs
 - monitoring [183](#)
- dis
 - permissions by command [258](#)
 - privileges by command [258](#)
- disable mode
 - PowerCenter Integration Services and Service Processes [52](#)
- domain
 - log event categories [167](#)
 - reports [200](#)
 - user activity, monitoring [200](#)
 - user security [51](#)
- domain configuration
 - description [60](#)
 - log events [167](#)
 - migrating [61](#)
- domain configuration database
 - backing up [61](#)
 - code page [227](#)
 - connection for gateway node [63](#)
 - description [60](#)
 - migrating [61](#)
 - restoring [61](#)
 - secure database [69](#)
 - updating [63](#)
- domain properties
 - Informatica domain [67](#)
- domain reports
 - License Management Report [200](#)
 - running [200](#)
 - Web Services Report [207](#)
- Domain tab
 - Connections view [38](#)
 - Informatica Administrator [30](#)
 - Navigator [30](#)
 - Services and Nodes view [30](#)
- domains
 - multiple [46](#)

E

- editing
 - connections [84](#)
- environment variables
 - LANG_C [225](#)
 - LC_ALL [225](#)
 - LC_CTYPE [225](#)
 - NLS_LANG [237](#), [240](#)
 - troubleshooting [54](#)

F

- Facebook connections
 - properties [91](#)
- failover
 - application service [76](#)
 - domain [76](#)
- flat files
 - connectivity [303](#)
 - exporting logs [165](#)
 - source code page [229](#)
 - target code page [230](#)
- folders
 - Administrator tool [49](#)
 - creating [49](#)
 - managing [49](#)
 - objects, moving [50](#)
 - overview [32](#)
 - removing [50](#)
- FTP
 - achieving high availability [81](#)

G

- gateway
 - managing [59](#)
- gateway node
 - configuring [59](#)
 - description [18](#)
 - log directory [59](#)
 - logging [159](#)
- gateways
 - states [192](#)
- GB18030
 - description [220](#)
- general properties
 - Informatica domain [67](#)
 - license [154](#)
- global settings
 - configuring [179](#)
- globalization
 - overview [219](#)
- graphics display server
 - requirement [200](#)
- Greenplum connections
 - properties [92](#)
- grids
 - dependencies [65](#)
 - Informatica Administrator tabs [37](#)
- groups
 - overview [41](#)
- Guaranteed Message Delivery files
 - Log Manager [158](#)

H

- hardware configuration
 - License Management Report [204](#)
- HBase connections
 - properties [94](#)
- HDFS connections
 - properties [95](#)
- high availability
 - description [23](#), [72](#)
 - failover [75](#)
 - recovery [77](#)
 - restart [75](#)
 - TCP KeepAlive timeout [81](#)
- high availability persistence tables
 - PowerCenter Integration Service [79](#)
- Hive connections
 - properties [96](#)
- HTTP connections
 - properties [101](#)

I

- IBM DB2
 - connect string syntax [306](#)
- IBM DB2 connections
 - properties [103](#)
- IBM DB2 for i5/OS connections
 - properties [105](#)
- IBM DB2 for z/OS connections
 - properties [108](#)
- IME (Windows Input Method Editor)
 - input locales [222](#)
- IMS connections
 - properties [111](#)
- incremental keys
 - licenses [150](#)
- Informatica Administrator
 - Domain tab [30](#)
 - logging in [25](#)
 - Logs tab [38](#)
 - Monitoring tab [39](#)
 - Navigator [40](#)
 - overview [29](#), [46](#)
 - Reports tab [39](#)
 - searching [40](#)
 - Security page [39](#)
 - service process, enabling and disabling [52](#)
 - Services and Nodes view [32](#)
 - services, enabling and disabling [52](#)
 - tabs, viewing [29](#)
- Informatica Analyst
 - connectivity [299](#)
- Informatica Cloud
 - Cloud Connections [244](#)
 - Cloud Organization Properties [243](#)
 - Cloud Organizations [242](#), [244](#)
 - Overview [242](#)
- Informatica Data Explorer
 - connectivity [299](#)
- Informatica Data Quality
 - connectivity [299](#)
- Informatica Data Services
 - connectivity [299](#)
- Informatica Developer
 - connectivity [299](#)

- Informatica domain
 - alerts [47](#)
 - database properties [68](#)
 - description [17](#)
 - domain configuration database [69](#)
 - domain properties [67](#)
 - general properties [67](#)
 - log and gateway configuration [69](#)
 - multiple domains [46](#)
 - permissions [51](#)
 - privileges [51](#)
 - restarting [66](#)
 - shutting down [66](#)
 - state of operations [77](#)
 - user security [51](#)
- Informatica My Support Portal
 - logging in [215](#)
- Information and Content Exchange (ICE)
 - log files [165](#)
- Informix
 - connect string syntax [306](#)
- input locales
 - configuring [222](#)
 - IME (Windows Input Method Editor) [222](#)
- Integration Service
 - connectivity [303](#)
 - ODBC (Open Database Connectivity) [298](#)
- ipc
 - permissions by command [259](#)
 - privileges by command [259](#)
- isp
 - permissions by command [260](#)
 - privileges by command [260](#)

J

- JDBC (Java Database Connectivity)
 - overview [307](#)
- JDBC connections
 - properties [114](#)
- JDBC drivers
 - Data Analyzer [298](#)
 - Data Analyzer connection to repository [305](#)
 - installed drivers [305](#)
 - Metadata Manager [298](#)
 - Metadata Manager connection to databases [305](#)
 - PowerCenter domain [298](#)
 - Reference Table Manager [298](#)
- JDBC-ODBC bridge
 - Data Analyzer [305](#)
- jobs
 - monitoring [181](#)

K

- Kerberos authentication
 - troubleshooting [26](#)

L

- LANG_C environment variable
 - setting locale in UNIX [225](#)
- LC_ALL environment variable
 - setting locale in UNIX [225](#)

- license
 - assigning to a service [152](#)
 - creating [151](#)
 - details, viewing [154](#)
 - general properties [154](#)
 - Informatica Administrator tabs [37](#)
 - keys [150](#)
 - license file [151](#)
 - log events [167](#), [169](#), [170](#)
 - managing [149](#)
 - removing [153](#)
 - unassigning from a service [152](#)
 - updating [153](#)
 - validation [149](#)
- license keys
 - incremental [150](#), [153](#)
 - original [150](#)
- License Management Report
 - CPU detail [202](#)
 - CPU summary [201](#)
 - emailing [206](#)
 - hardware configuration [204](#)
 - licensed options [205](#)
 - licensing [201](#)
 - multibyte characters [206](#)
 - node configuration [205](#)
 - repository summary [203](#)
 - running [200](#), [205](#)
 - Unicode font [206](#)
 - user detail [203](#)
 - user summary [203](#)
- license usage
 - log events [167](#)
- licensed options
 - License Management Report [205](#)
- licensing
 - License Management Report [201](#)
 - log events [169](#)
 - managing [149](#)
- licensing logs
 - log events [149](#)
- linked domain
 - multiple domains [46](#)
- LinkedIn connections
 - properties [117](#)
- Listener Service
 - log events [168](#)
- locales
 - overview [221](#)
- localhost_.txt
 - troubleshooting [159](#)
- Log Agent
 - description [157](#)
 - log events [167](#)
- log and gateway configuration
 - Informatica domain [69](#)
- log directory
 - for gateway node [59](#)
 - location, configuring [159](#)
- log errors
 - Administrator tool [166](#)
- log event files
 - description [158](#)
 - purging [160](#)
- log events
 - authentication [167](#)
 - authorization [167](#)
 - code [166](#)
- log events (*continued*)
 - components [166](#)
 - description [158](#)
 - details, viewing [161](#)
 - domain [167](#)
 - domain configuration [167](#)
 - domain function categories [166](#)
 - exporting with Mozilla Firefox [164](#)
 - licensing [167](#), [169](#), [170](#)
 - licensing logs [149](#)
 - licensing usage [167](#)
 - Log Agent [167](#)
 - Log Manager [167](#)
 - message [166](#)
 - message code [166](#)
 - node [166](#)
 - node configuration [167](#)
 - PowerCenter Repository Service [169](#)
 - saving [164](#)
 - security audit trail [169](#)
 - Service Manager [167](#)
 - service name [166](#)
 - severity levels [166](#)
 - thread [166](#)
 - time zone [160](#)
 - timestamps [166](#)
 - user activity [171](#)
 - user management [167](#)
 - viewing [161](#)
 - Web Services Hub [170](#)
 - workflow [196](#)
- Log Manager
 - architecture [158](#)
 - catalina.out [159](#)
 - configuring [161](#)
 - directory location, configuring [159](#)
 - domain log events [167](#)
 - log event components [166](#)
 - log events [167](#)
 - log events, purging [160](#)
 - log events, saving [164](#)
 - logs, viewing [161](#)
 - message [166](#)
 - message code [166](#)
 - node [166](#)
 - node.log [159](#)
 - PowerCenter Integration Service log events [169](#)
 - PowerCenter Repository Service log events [169](#)
 - ProcessID [166](#)
 - purge properties [160](#)
 - recovery [159](#)
 - SAP NetWeaver BI log events [170](#)
 - security audit trail [169](#)
 - service name [166](#)
 - severity levels [166](#)
 - thread [166](#)
 - time zone [160](#)
 - timestamp [166](#)
 - troubleshooting [159](#)
 - user activity log events [171](#)
 - using [157](#)
- Logger Service
 - log events [168](#)
- logical CPUs
 - calculation [201](#)
- logical data objects
 - monitoring [184](#)

- login
 - troubleshooting [26](#)
- logs
 - components [166](#)
 - configuring [159](#)
 - domain [167](#)
 - location [159](#)
 - PowerCenter Integration Service [169](#)
 - PowerCenter Repository Service [169](#)
 - purging [160](#)
 - SAP BW Service [170](#)
 - saving [164](#)
 - user activity [171](#)
 - viewing [161](#)
 - workflow [196](#)
- Logs tab
 - Informatica Administrator [38](#)
- lookup databases
 - code pages [231](#)

M

- managing
 - accounts [25](#)
 - user accounts [25](#)
- master gateway node
 - description [18](#)
- Maximum CPU Run Queue Length
 - node property [55](#)
- Maximum Memory Percent
 - node property [55](#)
- Maximum Processes
 - node property [55](#)
- Maximum Restart Attempts (property)
 - Informatica domain [53](#)
- message code
 - Log Manager [166](#)
- metadata
 - adding to repository [236](#)
 - choosing characters [236](#)
- Metadata Manager
 - connectivity [305](#)
 - ODBC (Open Database Connectivity) [298](#)
- Metadata Manager Service
 - application service [33](#)
 - code page [229](#)
 - custom roles [286](#)
 - log events [169](#)
- Microsoft SQL Server
 - connect string syntax [306](#)
- migrate
 - domain configuration [61](#)
- Model Repository Service
 - application service [33](#)
 - connectivity [299](#)
 - log events [169](#)
- monitoring
 - applications [182](#)
 - Data Integration Services [180](#)
 - deployed mapping jobs [183](#)
 - description [173](#)
 - global settings, configuring [179](#)
 - jobs [181](#)
 - logical data objects [184](#)
 - preferences, configuring [180](#)
 - reports [176](#)
 - setup [179](#)

- monitoring (*continued*)
 - SQL data services [185](#)
 - statistics [175](#)
 - web services [188](#)
 - workflows [189](#)
- Monitoring tab
 - Informatica Administrator [39](#)
- mrs
 - permissions by command [271](#)
 - privileges by command [271](#)
- ms
 - permissions by command [272](#)
 - privileges by command [272](#)
- MS SQL Server connections
 - properties [117](#)
- multibyte data
 - entering in PowerCenter Client [222](#)

N

- Navigator
 - Domain tab [30](#)
 - Security page [40](#)
- network
 - high availability [81](#)
- NLS_LANG
 - setting locale [237](#), [240](#)
- node configuration
 - License Management Report [205](#)
 - log events [167](#)
- node configuration file
 - location [54](#)
- node diagnostics
 - analyzing [218](#)
 - downloading [216](#)
- node properties
 - backup directory [55](#)
 - configuring [54](#), [55](#)
 - CPU Profile [55](#)
 - maximum CPU run queue length [55](#)
 - maximum memory percent [55](#)
 - maximum processes [55](#)
- node.log
 - troubleshooting [159](#)
- nodemeta.xml
 - for gateway node [59](#)
 - location [54](#)
- nodes
 - adding to Informatica Administrator [54](#)
 - configuring [55](#)
 - defining [54](#)
 - dependencies [65](#)
 - description [17](#), [18](#)
 - gateway [18](#), [59](#)
 - host name and port number, removing [55](#)
 - Informatica Administrator tabs [37](#)
 - Log Manager [166](#)
 - managing [54](#)
 - port number [55](#)
 - properties [54](#)
 - removing [59](#)
 - restarting [58](#)
 - shutting down [58](#)
 - starting [58](#)
 - TCP/IP network protocol [298](#)
 - worker [18](#)

O

- ODBC (Open Database Connectivity)
 - DataDirect driver issues [306](#)
 - establishing connectivity [306](#)
 - Integration Service [298](#)
 - Metadata Manager [298](#)
 - PowerCenter Client [298](#)
 - requirement for PowerCenter Client [304](#)
- ODBC connections
 - properties [120](#)
- oie
 - permissions by command [272](#)
 - privileges by command [272](#)
- operating mode
 - effect on resilience [80](#)
- Oracle
 - connect string syntax [306](#)
 - setting locale with NLS_LANG [237](#), [240](#)
- Oracle connections
 - properties [121](#)
- original keys
 - licenses [150](#)
- overview
 - connections [82](#)

P

- pass-through security
 - adding to connections [86](#)
 - connecting to SQL data service [85](#)
 - enabling caching [86](#)
 - web service operation mappings [85](#)
- password
 - changing for a user account [27](#)
- Percent Partitions in Use (property)
 - Web Services Report [208](#)
- permissions
 - as commands [257](#)
 - dis commands [258](#)
 - ipc commands [259](#)
 - isp commands [260](#)
 - mrs commands [271](#)
 - ms commands [272](#)
 - oie commands [272](#)
 - pmcmd commands [276](#)
 - pmrep commands [278](#)
 - ps commands [272](#)
 - pwx commands [273](#)
 - rtm commands [274](#)
 - sql commands [275](#)
 - wfs commands [276](#)
- pmcmd
 - code page issues [228](#)
 - communicating with PowerCenter Integration Service [228](#)
 - permissions by command [276](#)
 - privileges by command [276](#)
- PmNullPasswd
 - reserved word [304](#)
- PmNullUser
 - reserved word [304](#)
- pmrep
 - permissions by command [278](#)
 - privileges by command [278](#)
- port
 - application service [19](#)
 - node [55](#)
- port (*continued*)
 - node maximum [55](#)
 - node minimum [55](#)
 - range for service processes [55](#)
- PowerCenter
 - connectivity [298](#)
- PowerCenter Client
 - code page [228](#)
 - connectivity [304](#)
 - multibyte characters, entering [222](#)
 - ODBC (Open Database Connectivity) [298](#)
 - resilience [73](#)
 - TCP/IP network protocol [298](#)
- PowerCenter domains
 - connectivity [301](#)
 - TCP/IP network protocol [298](#)
- PowerCenter Integration Service
 - application service [33](#)
 - enabling and disabling [52](#)
 - failover configuration [79](#)
 - high availability persistence tables [79](#)
 - log events [169](#)
 - recovery [77](#)
 - recovery configuration [79](#)
 - resilience [74](#)
 - state of operations [77](#)
- PowerCenter Integration Service process
 - code page [228](#)
 - enabling and disabling [52](#)
 - restart, configuring [53](#)
 - supported code pages [245](#)
 - viewing status [57](#)
- PowerCenter Repository Service
 - application service [33](#)
 - connectivity requirements [303](#)
 - custom roles [284](#)
 - log events [169](#)
 - recovery [77](#)
 - resilience [74](#)
 - state of operations [77](#)
- PowerCenter security
 - managing [39](#)
- PowerExchange Listener Service
 - application service [33](#)
- PowerExchange Logger Service
 - application service [33](#)
- preferences
 - monitoring [180](#)
- privileges
 - as commands [257](#)
 - command line programs [257](#)
 - dis commands [258](#)
 - ipc commands [259](#)
 - isp commands [260](#)
 - mrs commands [271](#)
 - ms commands [272](#)
 - oie commands [272](#)
 - pmcmd commands [276](#)
 - pmrep commands [278](#)
 - ps commands [272](#)
 - pwx commands [273](#)
 - rtm commands [274](#)
 - sql commands [275](#)
 - wfs commands [276](#)
- process identification number
 - Log Manager [166](#)
- ProcessID
 - Log Manager [166](#)

ProcessID (*continued*)
message code [166](#)

ps
permissions by command [272](#)
privileges by command [272](#)
purge properties
Log Manager [160](#)
pwx
permissions by command [273](#)
privileges by command [273](#)

R

recovery
Data Integration Service [77](#)
high availability [77](#)
Integration Service [77](#)
PowerCenter Repository Service [77](#)
Reporting and Dashboards Service
application service [33](#)
Reporting Service
application service [33](#)
custom roles [287](#)
reports
Administrator tool [200](#)
domain [200](#)
License [200](#)
monitoring [176](#)
Web Services [200](#)
Reports tab
Informatica Administrator [39](#)
repositories
backup directory [55](#)
code pages [229](#)
supported code pages [245](#)
Unicode [220](#)
UTF-8 [220](#)
repository metadata
choosing characters [236](#)
repository summary
License Management Report [203](#)
resilience
application service [74](#)
application service configuration [78](#)
command line program configuration [80](#)
in exclusive mode [80](#)
PowerCenter Client [73](#)
PowerCenter Integration Service [74](#)
PowerCenter Repository Service [74](#)
TCP KeepAlive timeout [81](#)
resource provision thresholds
setting for nodes [55](#)
restart
application service [76](#)
configuring for PowerCenter Integration Service processes [53](#)
restoring
domain configuration database [61](#)
roles
overview [42](#)
rtm
permissions by command [274](#)
privileges by command [274](#)
run-time statistics
Web Services Report [210](#)

S

SAP BW Service
application service [33](#)
log events [170](#)
SAP connections
properties [124](#)
Search section
Informatica Administrator [40](#)
security
audit trail, viewing [169](#)
permissions [51](#)
privileges [51](#)
Security page
Informatica Administrator [39](#)
Navigator [40](#)
Sequential connections
properties [126](#)
Service Manager
authorization [18](#)
description [18](#)
log events [167](#)
service name
log events [166](#)
services and nodes
viewing dependencies [65](#)
Services and Nodes view
Informatica Administrator [32](#)
sessions
sort order [228](#)
severity
log events [166](#)
Show Custom Properties (property)
user preference [27](#)
shutting down
Informatica domain [66](#)
SMTP configuration
alerts [47](#)
sort order
code page [228](#)
source databases
code page [229](#)
sources
code pages [229](#), [247](#)
sql
permissions by command [275](#)
privileges by command [275](#)
SQL data services
monitoring [185](#)
stack traces
viewing [161](#)
state of operations
domain [77](#)
PowerCenter Integration Service [77](#)
PowerCenter Repository Service [77](#)
statistics
for monitoring [175](#)
Web Services Hub [207](#)
stopping
Informatica domain [66](#)
stored procedures
code pages [231](#)
Subscribe for Alerts
user preference [27](#)
subset
defined for code page compatibility [226](#)
superset
defined for code page compatibility [226](#)

Sybase ASE
 connect string syntax [306](#)
system locales
 description [221](#)

T

target databases
 code page [230](#)
targets
 code pages [230](#), [247](#)
tasks
 states [192](#)
TCP KeepAlive timeout
 high availability [81](#)
TCP/IP network protocol
 nodes [298](#)
 PowerCenter Client [298](#)
 PowerCenter domains [298](#)
 requirement for Integration Service [304](#)
Teradata
 connect string syntax [306](#)
testing
 database connections [84](#)
thread identification
 Logs tab [166](#)
threads
 Log Manager [166](#)
time zone
 Log Manager [160](#)
timestamps
 Log Manager [166](#)
troubleshooting
 catalina.out [159](#)
 code page relaxation [235](#)
 environment variables [54](#)
 Kerberos authentication [26](#)
 localhost_.txt [159](#)
 logging in [26](#)
 node.log [159](#)
Twitter connections
 properties [130](#)
Twitter Streaming connections
 properties [131](#)

U

UCS-2
 description [220](#)
Unicode
 GB18030 [220](#)
 repositories [220](#)
 UCS-2 [220](#)
 UTF-16 [220](#)
 UTF-32 [220](#)
 UTF-8 [220](#)
Unicode mode
 overview [222](#)
UNIX
 code pages [225](#)
UNIX environment variables
 LANG_C [225](#)
 LC_ALL [225](#)
 LC_CTYPE [225](#)
user accounts
 changing the password [27](#)

user accounts (*continued*)
 managing [25](#)
user activity
 log event categories [171](#)
user detail
 License Management Report [203](#)
user locales
 description [222](#)
user management
 log events [167](#)
user preferences
 description [27](#)
 editing [27](#)
user summary
 License Management Report [203](#)
users
 license activity, monitoring [200](#)
 overview [41](#)
UTF-16
 description [220](#)
UTF-32
 description [220](#)
UTF-8
 description [220](#)
 repository [229](#)

V

validating
 code pages [233](#)
 licenses [149](#)
viewing
 dependencies for services and nodes [65](#)
VSAM connections
 properties [132](#)

W

web connections
 properties [101](#)
Web content-Kapow Katalyst connections
 properties [134](#)
web services
 monitoring [188](#)
Web Services Hub
 application service [23](#), [33](#)
 log events [170](#)
 statistics [207](#)
Web Services Report
 activity data [208](#)
 Average Service Time (property) [208](#)
 Avg DTM Time (property) [208](#)
 Avg. No. of Run Instances (property) [208](#)
 Avg. No. of Service Partitions (property) [208](#)
 complete history statistics [211](#)
 contents [208](#)
 Percent Partitions in Use (property) [208](#)
 run-time statistics [210](#)
wfs
 permissions by command [276](#)
 privileges by command [276](#)
Within Restart Period (property)
 Informatica domain [53](#)
worker node
 configuring as gateway [59](#)
 description [18](#)

- workflow recovery
 - overview [195](#)
 - running [196](#)
- workflows
 - aborting [195](#)
 - canceling [195](#)
 - logs [196](#)
 - monitoring [189](#)
 - recovering [196](#)
 - states [191](#)

X

- X Virtual Frame Buffer
 - for License Report [200](#)
 - for Web Services Report [200](#)
- XML
 - exporting logs in [165](#)